2003-09

Navy/Marine Corps intranet information assurance operational services performance measures

Gumke, Randall A.; Gumke, Randall.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

NAVY/MARINE CORPS INTRANET INFORMATION ASSURANCE OPERATIONAL SERVICES PERFORMANCE MEASURES

by

Randall Gumke

June 2001

Thesis Advisor:	Daniel F. Warren
Associate Advisor:	Carl R. Jones

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	June 2001	Master's Thesis

4. TITLE AND SUBTITLE: Navy/Marine Corps Intranet Information Assurance Operational Services Performance Measures	5. FUNDING NUMBERS
6. AUTHOR(S) Gumke, Randall A.	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
Approved for public release; distribution is unlimited	A

13. ABSTRACT ***(maximum 200 words)***

Communicating in the Department of the Navy (DON) over the Internet is an everyday event. The DON is developing the Navy Marine Corps Intranet (N/MCI) to enhance this communication capability. The security of communicating over the N/MCI has become a concern to the DON. The DON is relying on the N/MCI contractor to provide security for their communications. Key aspects of this secure communication will be provided through the use of a DON Public Key Infrastructure (PKI), which the N/MCI contractor is managing. To ensure the security of the PKI based communications the contract requires the monitoring of four PKI performance measures. This thesis analyzes performance measures, criterion, and standards then uses this analysis to review the contractual PKI performance measures and data collected from commercial PKI vendors. It recommends changes to these performance measures and provides additional performance criteria that should be included in the N/MCI contract. Finally, this thesis analyses how the N/MCI contract, specifically the PKI, impact DON members.

14. SUBJECT TERMS Public Key Infrastructure, Public Key Cryptography, Navy Marine Corps Intranet, Service Level Agreements, Performance Measures, PKI, N/MCI	15. NUMBER OF PAGES 134
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

NAVY/MARINE CORPS INTRANET INFORMATION ASSURANCE OPERATIONAL SERVICES PERFORMANCE MEASURES

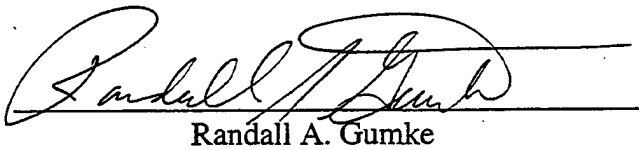
Randall A. Gumke
Lieutenant, United States Navy
B.S., University of Florida, 1993

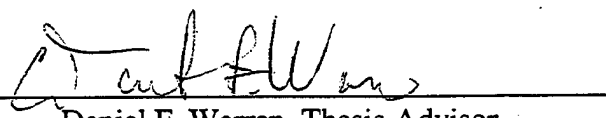
Submitted in partial fulfillment of the
requirements for the degree of

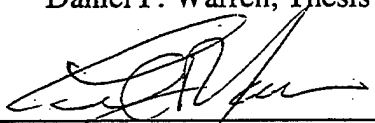
MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

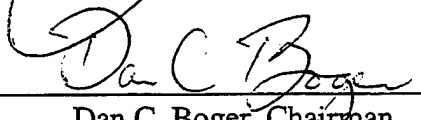
from the

NAVAL POSTGRADUATE SCHOOL
June 2001

Author: 
Randall A. Gumke

Approved by: 
Daniel F. Warren, Thesis Advisor


Carl R. Jones, Associate Advisor


Dan C. Boger, Chairman
Information Systems Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Communicating in the Department of the Navy (DON) over the Internet is an everyday event. The DON is developing the Navy Marine Corps Intranet (N/MCI) to enhance this communication capability. The security of communicating over the N/MCI has become a concern to the DON. The DON is relying on the N/MCI contractor to provide security for their communications. Key aspects of this secure communication will be provided through the use of a DON Public Key Infrastructure (PKI), which the N/MCI contractor is managing. To ensure the security of the PKI based communications the contract requires the monitoring of four PKI performance measures. This thesis analyzes performance measures, criterion, and standards then uses this analysis to review the contractual PKI performance measures and data collected from commercial PKI vendors. It recommends changes to these performance measures and provides additional performance criteria that should be included in the N/MCI contract. Finally, this thesis analyses how the N/MCI contract, specifically the PKI, impact DON members.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS

ATM	Asycronous Transfer Mode
BAN	Base Area Network
CA	Certification Authority
CONUS	Continental United States
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
DEERS	Defense Enrollment Eligibility Reporting System
DISA	Defense Information System Agency
DISN	Defense Information System Network
EDS	Electronic Data Systems Corporation
FIWC	Fleet Information War Center
FBCA	Federal Bridge Certification Authority
FPKI	Federal Public Key Infrastructure
IECA	Interim External Certificate Authority
IASE	Information Assurance Support Environment
LAN	Local Area Network
LRA	Local Registration Authority
MAN	Metropolitan Area Network
MCTN	Marine Corps Tactical Network
NSA	National Security Agency
NMCI	Navy Marine Corps Intranet
NIPRNET	Unclassified Internet Protocol Router Network
PEO-IT	Program Executive Officer for Information Technology
PKI	Public Key Infrastructure
PWC	Public Works Center
SIPRNET	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SPAWAR	Space and Naval Warfare Systems Command

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The author would like to thank my wife, Nan, and my daughter, Megan, for their unconditional love and support. They have understood and accepted my never ending studying. At the beginning of my Naval career, as a young sailor, I never dreamed that I would be writing a thesis and earning a graduate degree. Therefore, I would also like to thank the United States Navy for allowing me to pursue three college degrees during my 18 years of service.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PURPOSE

Communicating through the Internet is a common everyday practice that many members of the Department of the Navy (DON) perform without ever considering the possible security threats. In the near future when a member communicates sensitive material, it will be protected by cryptography that is based on the DON Public Key Infrastructure (PKI). Currently, the DON is transferring most of its information technology infrastructure to a commercial contractor. The Navy Marine Corps Intranet (N/MCI) contractor will take on the responsibility of managing the DON's PKI, as required by the N/MCI contract. [Ref. 2]

The N/MCI contract performance requirements for the PKI are described in Service Level Agreement (SLA) No. 34 which consists of four performance measurements:

- Certificate Revocation.
- Ability of one N/MCI user to obtain a certificate of another N/MCI user.
- Timeliness of user registration for a DOD certificate.
- Interoperability.

These performance measurements were rapidly developed by the N/MCI program managers, so that the contract could be written in a short period of time (six months) and quickly issued as a request for proposal [Ref. 3] The N/MCI program manager informed this author that, due to the limited time-line, the set of performance measurements were

produced are based, almost entirely, on intuition and not on commercial standards. This was due mainly to the lack of available information in a fairly new area of security. [Ref. 27] Since these performance measures were created quickly, this thesis will analyze them and compare them to performance measures from commercial PKI systems. [Ref. 27] Finally, this thesis makes recommendations to improve these performance measures using measurements, criterion and standards developed in this thesis.

With the entire DON shifting to a defense-in-depth strategy of information assurance, the DON is relying on PKI to be a major tier in this security platform. [Ref. 5] The importance of a properly operating PKI is understated and not reflected in the way that it was quickly written into the N/MCI contract. [Ref. 27] This thesis will emphasize the importance of ensuring that the PKI performance measures are complete and strong enough to create a secure atmosphere within the DON by analyzing them with measurements, criterion and standards developed in this thesis.

B. SCOPE AND METHODOLOGY

The objective for this thesis is to determine if the current contractual N/MCI PKI performance measures are satisfactory when compared to performance measures from commercial PKI systems.

An overview of the N/MCI contract is discussed first, followed by an analysis of performance measures, criterion, and standards. The results from this analysis are used to review the contract PKI performance measures and data collected from commercial PKI products. Finally, impacts to the DON due the award of the N/MCI contract are

discussed. (Readers unfamiliar with private/public key cryptology and PKI can refer to Appendix A.)

Research involved contacting commercial PKI vendors to determine how they measure the performance of their systems and what performance data they have collected for their systems. Finally, Space and Naval Warfare Systems Command (SPAWAR), who is in charge of monitoring the PKI performance measures, was contacted to obtain their insight regarding the quality of the contract requirements.

C. ORGANIZATION OF THESIS

There are six chapters and one appendix in this thesis. The first chapter gives an introduction to the thesis. The second chapter provides background information on the N/MCI contract. The third and fourth chapters are the analytical core of the thesis and answer the main thesis question. They present the results of the data collected during this research process and provide recommendations based on this analysis. The fifth chapter contains a study of the impact of the Navy Marine Corps Intranet on the fleet. The final chapter provides recommendations for future research in the PKI field. An appendix is provided with an overview of public/private key cryptography and PKI for readers who are not familiar with this material. The following is a summary of each chapter:

- Chapter I – Introduction. This chapter outlines the purpose of the thesis, thesis scope and methodology, and thesis organization.

- Chapter II – Navy Marine Corps Intranet Contract. This chapter analyzes the details of the N/MCI contract and the shortened award. It looks at the area of

coverage that N/MCI provides and the roles other government agencies play with N/MCI.

- Chapter III – Performance Measures, Criterion and Standards. In this chapter, performance measures, criterion, and standards are analyzed.

- Chapter IV – Performance Measures for N/MCI. This chapter analyzes the data collected using the characteristics developed in Chapter III. It compares commercial industry performance measures to the requirements outlined in the N/MCI contract and generates recommendations based on this analysis.

- Chapter V - Impact of N/MCI. This chapter discusses the N/MCI area of coverage and provides the costs and incentives the DON is paying for these services. It also examines the impact that the N/MCI implementation will have on the DON.

- Chapter VI – Conclusion. This chapter completes the thesis by providing recommendations of future research of PKI in the DOD.

- Appendix A – Public Key Cryptography and Public Key Infrastructure. This appendix provides a review of private and public key cryptography to form a basis for understanding a public key infrastructure. It also looks at the various components of PKI and how they interrelate

II. NAVY/MARINE CORPS INTRANET CONTRACT

A. GOAL OF THE N/MCI CONTRACT

Vice Admiral Richard Mayo, Director of Space, Information Warfare, and Command and Control clearly defined the goal of the Navy/Marine Corps Intranet (N/MCI) contract when he stated to Congress, on March 3, 2000, that the N/MCI is an "effort to achieve the most efficient, effective, and secure networked naval community we can." [Ref. 5] To reach these goals the N/MCI contract was conceived, developed, and awarded to outsource Unclassified Internet Protocol Router Network (NIPRNET) voice, data and video conferencing functions that the Navy and Marine Corps are presently handling themselves. N/MCI will also provide access points into the DOD's Secret Internet Protocol Router Network (SIPRNET) system.

The Navy states that their current system is inefficient and drastically impedes the sharing of information between Navy commands. Why? Under the current configuration, each command has its own independent systems and infrastructures. These independent systems have inadequate security measures and require extra resources to operate, maintain, and integrate with other commands. [Ref. 24] The Navy estimates that there are 477,900 data systems, 276,300 voice seats, and 490 video conferencing seats. [Ref. 25]

Under N/MCI, one contractor is responsible to maintain all of these systems and the networks connecting them. The Navy hopes that this contract will allow Navy and Marine Corps personnel to [Ref. 4]:

- Quickly and securely share knowledge around the globe.

- Reduce cost of voice, data, and video services.
- Eliminate interoperability issues.
- Remove access, connectivity, and throughput impediments to productivity and speed of command.
- Provide seamless migration and implementation of current infrastructure and applications into the N/MCI environment.

B. CONTRACTUAL ANALYSIS

1. Type of Contract

The contract is modeled after commercial style contracts. It requires no research and development, which, from the author's experience, hinders most DOD procurements. The Program Executive Officer for Information Technology (PEO-IT) implemented a streamlined approach for fielding the N/MCI contract. The PEO-IT created working partnerships with the Office of the Chief of Naval Operations (OPNAV), the Department of the Navy Chief Information Officer (DON CIO), the Deputy Assistant Secretary of the Navy for Command, Control, Communications, Computers and Intelligence (C4I) and the Marine Corps C4I offices. [Ref. 3] From these partnerships, the Naval requirements were quickly captured and developed into the contract within six months.

Most DOD contracts provide a product (end item). The N/MCI contractor, however, will provide a service to the Navy and Marine Corps. The Navy intends to turn over significant quantities of their information technology (IT) equipment to the contractor, who will maintain and upgrade it as indicated in the contract. The contract base period is five program years with an option for an additional three years. It was

awarded as a firm fixed price contract with performance incentives. [Ref. 3] These performance incentives strongly relate to the performance measures analyzed in this thesis and are discussed further in the Cost of Contract section of this chapter.

2. Award Determination

The government received four bids for the N/MCI contract. The government's qualification for award was not based on the "Low Bid", as was the case in the majority of past DOD contracts. The winner was selected based on technical competence and the "Best Value" concept. The contract was awarded to Electronic Data Systems Corporation (EDS) of Plano, Texas for $6,938,817,954. The guaranteed minimum for the five-year fixed price is $4,119,790,353, and for the three-year option period is $2,819,027,601 ($4,119,790,353 + $2,819,027,601 = $6,938,817,954). [Ref. 26] EDS can receive an additional $1.23M a year in incentive pay if they provide outstanding performance. [Ref. 2] An example of this potential incentive pay is the management of the public key infrastructure (PKI). This thesis analyzes the performance measures used to determine the amount of incentive pay.

C. AREA OF COVERAGE

The main purpose of the Navy Marine Corps Intranet is to provide services to as many of the Navy and Marine Corps personnel as possible. The N/MCI contract provides service to the entire Continental United States (CONUS), Alaska, Hawaii, Guantanamo Bay (Cuba), Puerto Rico, and Iceland. Because DON commands are dispersed across the world, they require a system that allows them to communicate securely. The basis for this secure communication is the N/MCI (PKI). This makes management of the PKI a key aspect of the N/MCI contract.

1. CONUS Assets

Presently, within the Navy and Marine Corps, each command operates their own Local Area Networks (LANs). These LANs connect to the government operated NIPRNET to provide connectivity between commands. The vision of the N/MCI is to incorporate local LANs into a larger Base Area Network (BAN) and then incorporate these BANs into a Metropolitan Area Network (MAN) as shown in Figure 2-1 As seen in this figure, a LAN is considered as an individual command located in a single area, such as a Public Works Center (PWC). Creating a BAN will entail connecting an entire base's LANs together. An example might be a Naval Amphibious (AMPHIB) Base. Finally, the MAN will collectively connect BANs within a specified region.

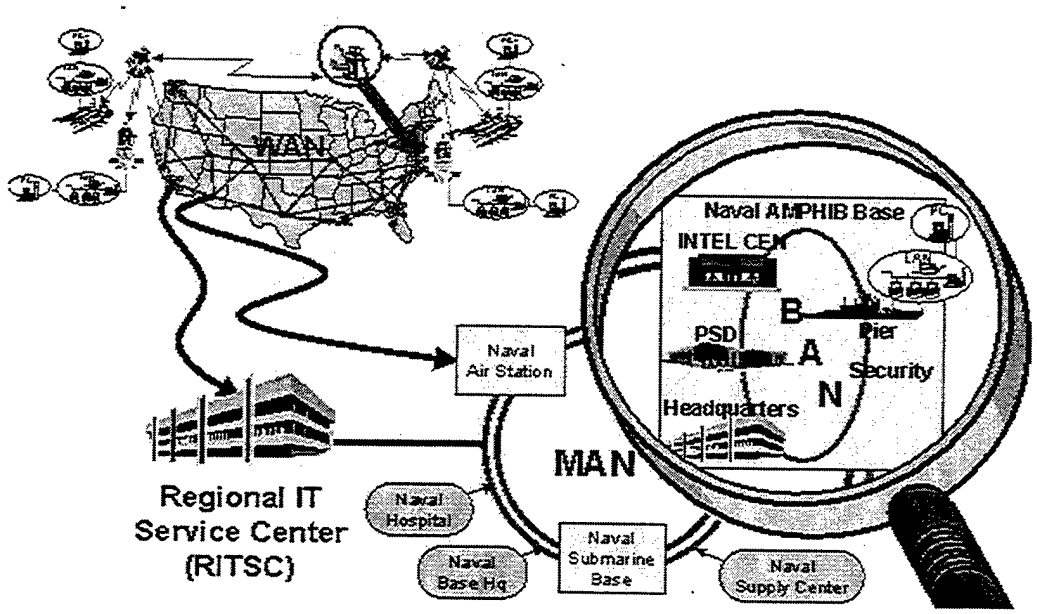


Figure 2-1. MAN & BAN. [From Ref. 15]

These networks will then be tied together into a Wide Area Network (WAN) that connects Navy and Marine Corps commands in the Continental United States and five areas outside CONUS as outlined above.

2. Deployed Assets

Under N/MCI, the contractor provides and manages computer workstation seats used by deployable commands. These deployable seats will interface with IT-21 shipboard networks and the Marine Corps Tactical Network (MCTN). The entire end-to-end solution is seen in Figure 2-2. These seats can be reconfigured by IT-21 personnel for deployments and, upon return, the N/MCI contractor will reconfigure the system back to N/MCI standards.

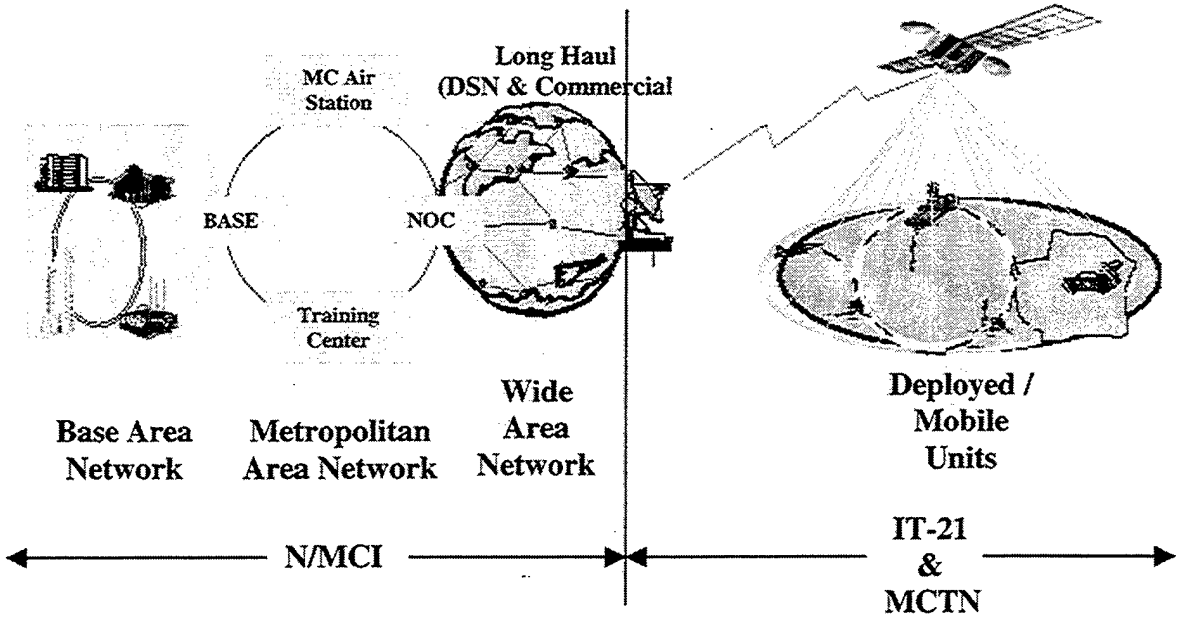


Figure 2-2. End-to-End Solution. [After Ref. 15]

With the increased development of shipboard Asycronous Transfer Mode (ATM) LANs, the demand for shore IT infrastructure will increase as well. The N/MCI provides the required infrastructure to meet this demand. [Ref 15] This end-to-end structure significantly enhances security, improves interoperability and increases access to information.

3. Defense-in-Depth

The DOD has decided to implement a Defense-in-Depth strategy to enhance Information Assurance (IA) within the military. The concept, as its title suggests, consists of layered security defenses that achieve the government's overall security objective. [Figure 2-3] Multiple locations within the network architecture provide functional security mechanisms. An example of Defense-in-Depth would be to have an e-mail software application wrapped with network protocol encryption. That result could be further protected by encrypting at the link layer. [Ref. 5]

The government anticipates that PKI will provide an enabling infrastructure for much of IA throughout the DOD and has stipulated that all DOD users are to be issued a Class 3 certificate by October 2002. [Ref. 10] PKI is an important part of the Navy's defense-in-depth strategy. This alone justifies the necessity to ensure the N/MCI PKI performance measures are correct and to standard, and is the purpose of this thesis.

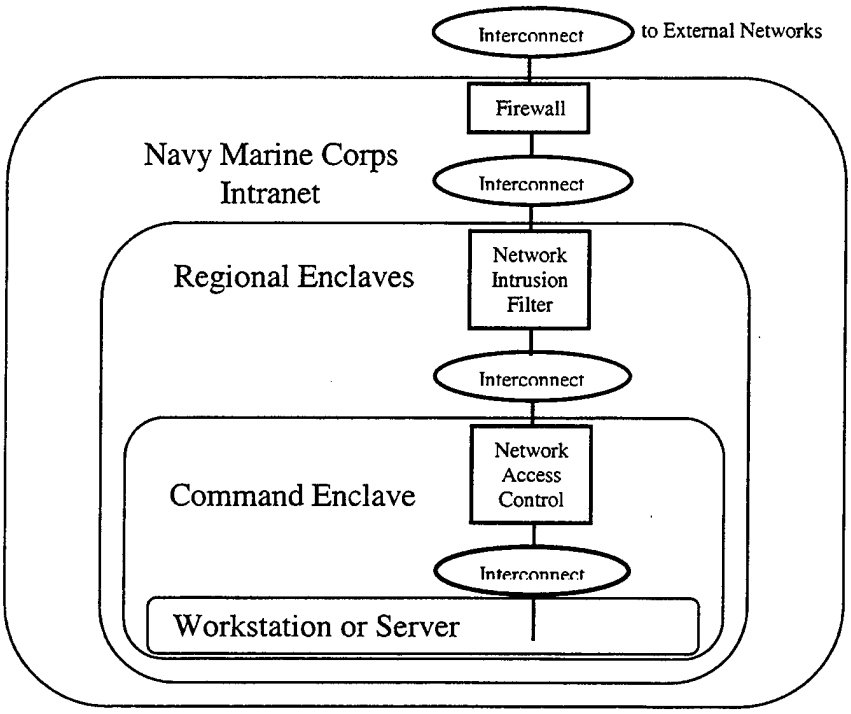


Figure 2-3. Defense in Depth. [From Ref. 5]

D. PAPERLESS CONTRACTING

One of the goals of the DON is to create a completely paperless contracting system. A true paperless contracting system would provide the following:

- Decrease the quantity of paper used in the contracting process.
- Decrease the number of contracting personnel.
- Create a more efficient and faster contracting system.

The biggest concern in going paperless is accountability. To provide accountability contracts are digitally signed when transmitted over the Internet. The digital signature of a document obtained over the Internet provides a way of establishing unequivocally that an individual has signed that purchase order and prevents them from later denying the fact. In essence, it is a contract between the sender and the receiver.

This thesis analyzes the performance measures involved in ensuring EDS correctly and in a timely manner creates and manages the infrastructure required for these digital signatures. Digital signatures are discussed in more detail in Appendix A.

E. GOVERNMENT AGENCIES' ROLES

There is an extremely large number of agencies involved in N/MCI, with each playing some role in this new contract. Table 2-1 outlines the responsibilities of each of agency to give the reader some reference on how they impact the contract.

Table 2-1 Government Agencies Connected with N/MCI

SPAWAR – Space and Naval Warfare Systems Command – SPAWAR provides the actual post award contracting and program management. SPAWAR will provide the green team involved in verifying that the contractor is in compliance with security-related service level agreements.
DISA - Defense Information Systems Agency – As discussed above DISA will provide long-haul voice, video and data network to EDS.
NAVSEA – monitors the overall contract.
FIWC – Fleet Information Warfare Center – FIWC will lead the Red Teams that will focus on general system vulnerabilities and evolving threats.
NCTF-CND: Navy Component Task Force for Computer Network Defense – This entity monitors cyber intrusions against Pentagon networks.
NSA –National Security Agency – NSA is the root certificate authority for the PKI of the N/MCI.

The list in Table 2-1 was created from the information gathered in researching this thesis. It should not be considered inclusive of all government agencies involved in monitoring the N/MCI contract. This thesis analyzes SPAWAR's role in monitoring N/MCI's PKI performance measures.

III. PERFORMANCE MEASURES, CRITERION & STANDARDS

A. INTRODUCTION

In this chapter performance measures, criterion, and standards are analyzed. A performance measure is a variable that indicates the behavior of a system. A criterion is a threshold value of the performance measure that indicates the acceptable level of performance. A standard is the combination of a performance measure and a criterion. This chapter's content focuses on the necessary concepts for understanding measures, criteria, and thus standards. Specific standards are suggested for Intranets in general and the Navy/Marine Corps Intranet (N/MCI) in particular. Finally, standards from commercial PKI vendors are provided.

B. PERFORMANCE MEASURES

1. Performance Measures

Performance measures for an Intranet and specifically the N/MCI are discussed below. [Ref. 1]

- Meaningful – The performance measure must be relevant to the DON's overall mission and their goals. This is measured as follows:
    - Time to revoke a certificate.
        - Measure: It is measured from when a member informs the Certificate Authority (CA) that their certificate has been compromised and needs to be revoked, until the certificate is actually on the Certificate Revocation List.

- Scale: Table 3-1 illustrates the probability of a command successfully completing their mission based on the amount of time taken to revoke a certificate. Note: This scale and the following scales are illustrations and should not be considered as factual.

Table 3-1. Mission Success Based on Certificate Revocation Time.

Minutes	Probability of Mission Success
1 to 5	100%
6 to 10	75%
11 to 15	50%
16 to 20	25%
20 and up	0%

- Criterion: If a command wants to achieve a 75% chance of having a successful mission, the certificate should be revoked within 6 to 10 minutes.

o Time to retrieve a user's public key.

- Measure: It is measured from when a user enters their request for the public key until the user receives the public key.

- Scale: Table 3-2 illustrates the probability of a command successfully completing their mission based on the amount of time taken to retrieve a user's public key.

Table 3-2. Mission Success Based on User's Public Key Retrieval Time.

Minutes	Probability of Mission Success
1 to 5	100%
6 to 10	75%
11 to 15	50%
16 to 20	25%
20 and up	0%

- Criterion: If a command wants to achieve a 75% chance of having a successful mission, a user's certificate should be received within 6 to 10 minutes.

- Time to create a new certificate.
  - Measure: It is measured from when a new user initiates the certificate request until the certificate is received.
  - Scale: Table 3-3 illustrates the probability of a command successfully completing their mission based on the amount of time taken to create a new certificate.

Table 3-3. Mission Success Based on New Certificate Creation Time.

Hours	Probability of Mission Success
1 to 8	100%
9 to 24	75%
25 to 72	50%
73 to 120	25%
121 and up	0%

- Criterion: If a command wants to achieve a 75% chance of having a successful mission the new certificate should be created within 9 to 24 hours.

- Interoperability issues impacting the mission.
  - Measure: It is measured by determining which networks give commands interoperability problems.
  - Scale: Table 3-4 illustrates the probability of a command successfully completing its mission based on the ability to operate with other networks.

Table 3-4. Mission Success Based on Interoperability Between Networks

Cannot Interoperate With	Probability of Mission Success
Civilian Networks	100%
DOD Networks	75%
DON Wide Area Networks	50%
DON Base Area Networks	25%
DON Local Area Networks	0%

  - Criterion: If a command wants to achieve a 75% chance of having a successful mission they need to be able to operate with DOD networks.
  - Measure: It is measured by determining how long the command is not mission-capable because the system inoperable.

- Scale: Table 3-5 illustrates the probability of a command successfully completing its mission based on the system down-time.

Table 3-5. Mission Success Based on Time that a Command is Inoperable

System Inoperable (Down-time) (in hours)	Probability of Mission Success
0 – 1	100%
2 – 5	75%
6 – 24	50%
25 - 72	25%
73 and up	0%

- Criterion: If a command wants to achieve a 75% chance of having a successful mission, the system should not be inoperable longer than 5 hours.

- Responsibility Related – The performance measure must be taken by a department or other organization entity that can guarantee the data has not been modified. To ensure that the data has not been modified, the following three areas will be measured:
  - The qualifications of the person performing the measurement.
    - Measure: What are the person's knowledge, skills, and competence in taking Intranet performance measures?
    - Scale: The scale in Table 3-6 is used to determine if the person taking the performance measure has the necessary

qualifications. A Likert scale is used with numbers to measure the order of the qualifications.

Table 3-6. Qualifications for Performing the Measurement

Oualifications	Scale
Very Knowledgeable/Very Skillful/ Very Competent	100
Very Knowledgeable/Very Skillful/Competent	75
Very Knowledgeable /Skillful/Competent	50
Knowledgeable/Skillful/Competent	25
No Qualifications	0

- Criterion: To receive a value of 75, the person performing the measurement must be very knowledgeable, very skillful and competent.

- Does the data from the performance measurement determine organizational and contractual incentives.

  - Measure: What are the potential rewards to the measuring organizational entity as a result of the information obtained by processing the data collected?

  - Scale: The scale in Table 3-7 is used to determine if gathering performance measurements provides an incentive. An incentive can be in the form of money or some form of compensation, such as time off. A Likert

scale is used with numbers to measure the order of the incentives.

Table 3-7. Type of Incentives for Performing the Measurement

Incentives	Scale
Monetary Incentives	100
Other Incentives	75
No Incentive	0

- Criterion: To receive a value of 75, the person performing the measurement is receiving some form of incentive other than monetary.

- The person performing the measurement has the ability to collect the data.
  - Measure: What is the person's ability in taking performance measurements? This ability is based on the number of years of experience performing the measurement.
  - Scale: The scale in Table 3-8 is used to determine if a person has the ability to collect the performance measurement data. A Likert scale is used with numbers to measure the order of their abilities.

Table 3-8. Ability of Person Performing the Measurement

Ability (Performed Measurement how many years)	Scale
Over 10	100
5 to 10	75
3 to 4	50
1 to 2	25
0	0

- Criterion: To receive a value of 75, the person performing the measurement must have performed this measurement for at least 5 years but not more than 10 years.

- Time Interval – The performance measurement is collected and reported within a reasonable time interval. The specific attribute is analyzed for:
  - How often is the measurement is taken?
    - Measure: It is measured by the time interval between performing sequential measurements.
    - Scale: The scale in Table 3-9 is used to determine if the collection of performance measurement data is accomplished in a timely manner. A higher number indicates a more preferable selection.

Table 3-9. Interval Between Data Collection.

Interval Between Data Collection	Timeliness
Continuouslv	5
Daily	4
Weekly	3
Monthly	2
Randomly	1

- Criterion: To receive a value of 4, the interval between sequential data collection is one day.

- How often are reports of collected data provided.

  - Measure: It is measured by the interval between providing sequential reports.

  - Scale: The scale in Table 3-10 is used to determine if the performance measurement report is provided in a timely manner. A higher number indicates a preferable selection.

Table 3-10. Interval Between Reports.

Interval Between Reports	Timeliness
Continuouslv	5
Daily	4
Weekly	3
Monthly	2
Randomly	1

  - Criterion: To receive a value of 4, the interval between sequential reports is one day.

- Credible – The data from the performance measurement is accurate and reliable. The specific attribute is analyzed for:
    - Is the data accurate?
        - Measure: Accuracy is measured by the size of the confidence interval based on a fixed confidence level. A smaller interval is preferable.
        - Scale: Size of the interval.
        - Criterion: If the data collected has the same confidence level, the data with the smallest interval should be the most accurate.
    - Is the data reliable?
        - Measure: Reliability is measured by the size of the confidence interval based on a fixed confidence level. A smaller interval is preferable.
        - Scale: Size of the interval.
        - Criterion: If the data collected has the same confidence level the data with the smallest interval should be the most reliable.
- Cost Effective – Is the measurement process efficient? The specifics are:
    - Are there other ways to measure the data?

        - Measure: It is measured by the number of alternatives considered.
        - Scale: Number of alternatives.
        - Criterion: Consideration of more alternatives is an indication of a more efficient measurement process.

- Comparable – The measured data is evaluated with previously collected data under the same conditions and the definition of the variable is constant. The specific attribute is analyzed for:
    - Have the conditions changed?
        - Measure: Verify that the conditions have/have not changed.
        - Scale: Yes or No.
        - Criterion: If the conditions have not changed the data collected can be used for comparison.
    - Has the definition of the variable changed?
        - Measure: Verify that the definition for the variable has/has not changed.
        - Scale: Yes or No.
        - Criterion: If the definition of the variable has not changed the data collected can be used for comparison.

The above criteria is used in the following sections to analyze the performance measures stated in the N/MCI contract.

2. PKI Measures Capabilities from Commercial Sources

The concept of Public Key Infrastructures has been around for nearly 30 years, however, the actual commercial adoption of PKIs has accelerated within the last four to five years. This recent commercial interest in PKIs is due to the success of E-commerce as a daily tool. [Ref. 27] In conducting the research for this thesis, the author discovered that PKI's short history has not permitted the development of a large number of performance measures. This will limit the government's ability to measure performance. In addition, the deployment of PKI has been mainly in smaller businesses (relative to the Department of the Navy) where they do not routinely monitor the certificate revocation, certificate creation or any interoperability issues. [Ref. 27] However, the performance measures that have been developed are applicable to any scale of intranet operations.

To obtain current data on commercially used PKI performance measures, twenty different vendors were contacted via e-mail. Only six vendors replied to the questions of how they measured their public key infrastructure performance. Vendors were specifically questioned on the four categories in the N/MCI PKI service level agreement. The Gartner Co., who specializes in collecting data to help organizations improve their business, was also contacted, but they could not provide any data on PKI performance measures. [Ref. 36] The following is a compilation of the performance measures that were obtained during the research for this thesis:

a. Certificate Revocation

The actual revocation can be completed by the Certificate Authority/Registration Authority/Local Registration Authority (CA/RA/LRA) within a few seconds for most PKI systems. [Ref. 29]. However, the actual certificate revocation list (CRL) update is dependent upon the transfer frequency of the CRL to the servers. For example the complete CRL could be transferred to all servers every four hours, with an incremental update every ten minutes. [Ref. 35] Below are the performance measure data collected from various companies for certificate revocation.

CertCo Inc.: The CA can update the CRL within 60 seconds. [Ref. 29]

Information Assurance Support Environment (IASE): As long as the RA has all the necessary information to identify the certificate and they have access to the directory, it should be within 30 seconds. [Ref 30]

Litronic Inc.: The CA can update the CRL within 5 to 10 minutes. [Ref. 31]

Netlock Technologies Inc.: This company refers to their CA's as managers and the certificate users as agents. When they revoke a certificate from the agent, the revocation is within 30 seconds, if the manager is online. If the manager is offline, the system will keep trying to contact the manager until they are online. [Ref. 32]

Eccelerate.com: As soon as the end-user accesses their website and puts in a revocation request, the request is processed and the certificate is revoked. They do not address the issue of CRLs and the time required for the revoked certificate to be placed on the lists. [Ref 33]

Digital Signature Trust Co.: Revocation can be accomplished within 1 minute by calling their Help Desk or Registration office. However, the update to the certificate revocation list is only every 24 hours for their Interim External Certificate Authority (IECA) program with the DOD. [Ref. 34]

b. Ability of One User to Obtain a Certificate of Another User

This performance measure is dependent on how users obtain certificates for other users' public keys. They can obtain the certificate either through an attachment in an e-mail, through a Lightweight Directory Access Protocol (LDAP), or through a key server. It is also dependent on whether the certificate is coming from directories that are shared between the two customers. [Ref. 29] Below are the performance measure data collected from various companies and commands in retrieving public keys.

CertCo Inc.: Certificates can be obtained within 60 to 90 seconds, dependent on what method is used to provide public keys to other members. [Ref. 29]

IASE: As long as the directory is available, a user can obtain a certificate within 60 seconds. [Ref. 30]

Litronic Inc.: Certificates can be obtained within 3 to 5 minutes. [Ref. 31]

Netlock Technologies Inc.: This company refers to their CA's as managers and the certificate users as agents. Communication between agents to obtain their public keys occurs within 5 seconds. [Ref. 32]

Eccelerate.com: Certificates can be obtained within 5 to 10 seconds. [Ref. 33]

Digital Signature Trust Co.: Among the IECA vendors, these public keys can be obtained within 10 seconds. [Ref. 34]

c. Time to Register

The time it takes to create a public key certificate (and get a private key) depends upon the time it takes to enter the user information, and the time it takes to receive the private key securely.

The length of time it takes for the requester to input the information will vary depending on if it is a web-based system or if an individual would have to physically go somewhere. Although all registration methods require user authentication at a registration workstation, there are different methods for generating and distributing the private key. The private key has to be delivered to the individual by some secure means. This could be through a rapid secure socket layer (SSL) web page or through a lengthy process of physically accepting the private key from the registration authority. [Ref. 6]

Smart Card technology will provide a member with instantaneous certificate creation after the first-time-use of the card. The user will still have to authenticate their identity with the registration authority issuing the Smart Cards. The cards will be distributed through DEERS (Defense Enrollment Eligibility Reporting System) and will only take eight minutes longer than issuing the current DOD ID card. [Ref. 37] Below are the performance measure data collected from various companies for certificate creation.

CertCo Inc.: Depending on what system is in place to qualify a member, it could take from 5 minutes to 5 days to create a certificate. [Ref. 29]

IASE: It can take from 5 to 10 minutes from when the LRA uploads the information until the member receives the certificate. [Ref. 30]

Litronic Inc.: Certificates can be created within 5 to 10 minutes depending on the profile that you want to store on the individual. [Ref. 31]

Netlock Technologies Inc.: This company refers to their CA's as managers and the certificate users as agents. When an agent is online while the manager is also online, it will only take 1 minute for an agent to receive a certificate. [Ref. 32]

Eccelerate.com: They advertise that 70% of their requests are completed within 2 business days. [Ref. 33]

Digital Signature Trust Co.: It can take from 10 to 14 days to create a certificate. [Ref. 34]

d. Interoperability

The companies contacted during this thesis offer a complete package for a single small enterprise. These standalone systems have very few interoperability issues. However, the DON will need to be completely interoperable with itself and other government agencies. Below are the performance data collected from various companies and commands for interoperability.

CertCo Inc.: Their systems support the PKI X.509 industry standard, however, they will always try to accommodate any product. [Ref. 29]

IASE: Their system will be fully interoperable with all vendors once they implement the Federal Bridge Certificate Authority (BCA). [Ref. 30] (BCA is discussed further in the next section.

Litronic Inc.: Their system supports PKI X.509. [Ref. 31]

Netlock Technologies Inc.: Their system is operable with many industry standards. [Ref. 32]

Eccelerate.com: Their systems support all the industry standards. [Ref. 33]

Digital Signature Trust Co.: For the IECA vendors the program requires that it work only with Netscape. The applications that their PKI systems intend to support are the Defense Travel Service (DTS), Electronic Data Access (EDA), Military Traffic Management Control (MTMC), and Paperless Contracting Wide Area Workflow (WAWF). [Ref. 34]

As indicated above, the PKI commercial industry provides very few performance measures for their systems. They also do not provide information concerning criterion of a specific measure. The performance measure data from commercial vendors was collected from test labs and not from testing their systems on customer's systems. PKI companies claim to provide information on how secure their program makes your communications, however, they do not provide complete performance measures on the issues discussed in this thesis. The author believes that these performance measures are not monitored by vendors, because the cost to perform this monitoring outweighs the benefits of the data collected.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. PERFORMANCE MEASURES, CRITERIA, AND STANDARDS FOR N/MCI

A. INTRODUCTION

This chapter discusses the application of performance measures for the N/MCI in Service Level Agreement (SLA) 34 Performance Measures for Information Assurance Operational Services, Public Key Infrastructure (PKI). It provides a list of the contractual requirements for these performance measures. This chapter takes the contractual performance measures and analyzes them based on the characteristics outlined in Chapter III. From the analysis, recommendations and the costs for these recommendations are provided. The last section analyzes how these performance measures will provide an incentive for the N/MCI contractor to perform at or above the contract requirements for PKI

B. APPLICATION OF PERFORMANCE MEASURES TO N/MCI

Measuring performance means setting the goal, measuring performance, comparing these two and choosing a corrective action. [Ref. 1] Performance measures are the standards the government will employ to evaluate the contractor's progress. SLA 34 of the N/MCI contract consists of four performance measurements: [Ref. 2]

- Certificate Revocation.
- Ability of one N/MCI user to obtain a certificate of another N/MCI user.
- Timeliness of user registration for a DOD certificate.
- Interoperability.

The N/MCI contractor is required to supply the DON with data collected while taking or recording the above performance measures.

1. Basis of Performance Measures

As indicated in Chapter II of this thesis, the Navy/Marine Corps Intranet contract was modeled after commercial style contracts. This was done so that the contract could be written in a short period of time (six months) and quickly issued as a request for proposal. [Ref. 3] This short-fused project did not allow sufficient time for the N/MCI program office to successfully research the performance measures required for Public Key Infrastructure systems. While interviewing the N/MCI program manager, he stated that his team could not find any commercial precedents for security measures, specifically PKI performance measures. The team had to work from common sense identification of measurable attributes in an attempt to balance what they expected from the contractor with what users needed in terms of responsiveness. [Ref. 27] The research phase of this thesis also discovered very few commercially available public key infrastructure performance measures.

2. N/MCI Contract Performance Measures

Performance measures in the public key infrastructure section of the N/MCI contract are used to examine the ability of the contractor to properly and efficiently manage certificates, and determine how well their systems interoperate with other systems. Tables 4-1 through 4-4 show the four performance measures for Service Level Agreement (SLA) No. 34 "Information Assurance Operation Services – PKI". Each table contains the requirements for a specific performance measure that are the responsibility of the contractor. It indicates who is responsible for monitoring the category, how it shall

be measured, and at what frequency it is monitored. Each table also indicates three levels of service that every command may choose from based on their individual requirements. The levels of service are:

Level of Service (1): Basic.
Level of Service (2): High End.
Level of Service (3): Mission Critical.

The requirements in the following tables are analyzed in the next section to determine if these performance values are sufficient to meet the demands of the DON.

Table 4-1. Performance Category 1: Certificate Revocation. [After Ref. 2]

Performance Measure Description: Timeliness of revoking a certificate when required.				
Who: Vendor & Government		Frequency: Continuous by vendor, random by government		
Where: Operations Center		How measured: Elapsed time from notification of the NMCI contractor that a user certificate needs to be revoked, to the notification of the certification authority		
	B Value (Unclassified)	B Value (Classified)	Pre-Negotiation	Contract SLA
Level of Service (1)	1 hour	30 minutes	1 hour / 30 minutes	1 hour / 30 minutes
Level of Service (2)	1 hour	30 minutes	1 hour / 30 minutes	1 hour / 30 minutes
Level of Service (3)	1 hour	30 minutes	1 hour / 30 minutes	1 hour / 30 minutes

Table 4-2. Performance Category 2: Ability of one NMCI user to obtain the DOD Public Key Infrastructure X.509 certificate of another NMCI user for purposes of sending electronic mail. [After Ref. 2]

Performance Measure Description: Time required for users to successfully obtain on the first attempt the X.509 certificates from the NMCI Public Key Infrastructure. The percentage applied is the rate at which users successfully obtain the certificate within the specified time period.				
Who: Vendor		Frequency: Monthly report		
Where: Operations Center		How measured: The time it takes for users to successfully obtain X.509 certificates when attempted. The stipulated target time (and percentage) to obtain certificates varies by level of service and unclassified/classified.		
	B Value (Unclassified)	B Value (Classified)	Pre-Negotiation	Contract SLA
Level of Service (1)	5 minutes, 99.7%	2 minutes, 99.9%	5 min, 99.7% / 2 min, 99.9%	5 min, 99.7% / 2 min, 99.9%
Level of Service (2)	5 minutes, 99.7%	2 minutes, 99.9%	5 min, 99.7% / 2 min, 99.9%	5 min, 99.7% / 2 min, 99.9%
Level of Service (3)	5 minutes, 99.7%	2 minutes, 99.9%	5 min, 99.7% / 2 min, 99.9%	5 min, 99.7% / 2 min, 99.9%

Table 4-3. Performance Category 3: User registration for DOD Public Key Infrastructure within N/MCI. [After Ref. 2]

Performance Measure Description: Measures the time from the submission of a user request to establishing fully functional DOD PKI X.509 certificates. The calculation is the number achieved divided by the number requested within a specified time.				
Who: Vendor		Frequency: Monthly report		
Where: DON-wide		How measured: The time it takes from submission of a user request for a DOD PKI X.509 certificate to being fully functional using DOD PKI within NMCI.		
	B Value (Unclassified)	B Value (Classified)	Pre-Negotiation	Contract SLA
Level of Service (1)	85% (1 week), 100% (2 week)	85% (1 week), 100% (2 week)	85% (1 wk), 100% (2 wk) / 85% (1 wk), 100% (2 wk)	85% (1 wk), 100% (2 wk) / 85% (1 wk), 100% (2 wk)
Level of Service (2)	85% (1 week), 100% (2 week)	85% (1 week), 100% (2 week)	85% (1 wk), 100% (2 wk) / 85% (1 wk), 100% (2 wk)	85% (1 wk), 100% (2 wk) / 85% (1 wk), 100% (2 wk)
Level of Service (3)	90% (3 days), 100% (1 week)	90% (3 days), 100% (1 week)	90% (3 days), 100% (1 wk) / 90% (3 days), 100% (1 wk)	90% (3 days), 100% (1 wk) / 90% (3 days), 100% (1 wk)

Table 4-4. Interoperability. [After Ref. 2]

<table>
<tr><td colspan="4">Performance Measure Description: This service requires full interoperability and seamless interface both within NMCI and to external and non-NMCI customers. The purpose of this metric is to indicate the vendor's level of compliance in measurable terms. The vendor will develop an interoperability test plan and procedures that support this particular service. The test plan reporting criteria will include a threshold level, agreed to by Government and the vendor, that requires immediate notification of the Government and appropriate action by the vendor to correct. Implementation of the approved test plan is required as part of standard NMCI operational procedures. Metrics indicated below reflect a standard criteria for the vendor to report to Government upon exceeding the threshold value agreed upon and stated in the interoperability test plan.</td></tr>
<tr><td colspan="2">Who: Vendor</td><td colspan="2">Frequency: Measured continuously, summarized daily, reported monthly, or when plan threshold value exceeded</td></tr>
<tr><td colspan="2">Where: Appropriate to this service (identified in test plan)</td><td colspan="2">How measured: Measured by Help Desk data or at points appropriate to this service category, as specifically identified in the NMCI interoperability test plan.</td></tr>
<tr><td></td><td>B Value</td><td>Pre-Negotiation</td><td>Contract SLA</td></tr>
<tr><td>Level of Service (1)</td><td></td><td>within 1 day</td><td>within 1 day</td></tr>
<tr><td>Level of Service (2)</td><td></td><td>within 1 day</td><td>within 1 day</td></tr>
<tr><td>Level of Service (3)</td><td></td><td>within 4 hours</td><td>within 4 hours</td></tr>
</table>

3. Analyzing the contact performance measures

The criteria outlined in Section B of Chapter III above is used to analyze the N/MCI contract performance measures.

a. Certificate Revocation

Description: The time it takes from when a certificate becomes compromised until it has been revoked. The N/MCI certificate revocation performance measure is analyzed below using the analytical concepts from Chapter III. First the contract values are provided, then the scale from the analytical concepts in Chapter III is used to determine if the measurements meet the standards. Finally, the data collected for this measure will be analyzed using the analytical concepts from Chapter III.

- Meaningful:
    - Contract Value: The contract requires that a certificate must be revoked within 1 hour (30 minutes for classified certificates).
    - Probability of Mission Success: Comparing the contract value above to the scale in Table 3-1, a value of 0% is obtained.

    Note: This value and the following values are derived from scales developed in Chapter III as illustrations and should not be considered as factual.

  - Comparison:
    - Commercial Vendors: The data from Section B2 of Chapter III indicates that commercial certificates are revoked within 1 minute to 24 hours
    - Probability of Mission Success: Comparing the commercial values above to the scale in Table 3-1, values of 100% to 0% are obtained.

This data indicates that the revocation performance measure is not within commercial standards and will affect the performance of a command's mission.

- Responsibility Related:
    - Qualifications:
        - Contract Value: The contract does not specify the qualifications of the person performing this measure.
        - Scale: Comparing the contract value above to the scale in Table 3-6, a value of 0 is obtained.
    - Comparison:
        - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not require any qualifications for the person performing this measurement.
        - Scale: Comparing the commercial value above to the scale in Table 3-6, a value of 0 is obtained.
    - Incentive for data:
        - Contract Value: The contract indicates that the contractor will receive monetary incentives for performance values within contract requirements.
        - Scale: Comparing the contract value above to the scale in Table 3-7, a value of 100 is obtained.
    - Comparison:

- Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not have to provide any incentive for performing this measure.
- Scale: Comparing the commercial value above to the scale in Table 3-7, a value of 0 is obtained.

- Ability of person collecting data.
  - Contract Value: The contract does not specify the ability of the person performing this measure.
  - Scale: Comparing the contract value above to the scale in Table 3-8, a value of 0 is obtained.
- Comparison:
  - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not require any qualifications for the person performing this measure.
  - Scale: Comparing the commercial value above to the scale in Table 3-8, a value of 0 is obtained.

This data illustrates that the contract does not require a person who is qualified to perform the measurement. It also indicates that the contractor will receive incentive pay for producing data that is within the contract requirements.

- Time Interval:
    - Contract Value: The contract requires continuous monitoring and reporting of the revocation of certificates to the DON.
    - Timeliness: Comparing the contract value above to the scale in Tables 3-9 and 3-10, values of 5 for monitoring and 5 for reporting are obtained.
  - Comparison:
    - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not monitor this criterion for the certificate revocation performance measure.
    - Timeliness: Since vendors do not monitor this measure, no comparison can be made between the vendor's value and the scale established in Chapter III.

This data illustrates that continuous monitoring is necessary for the revocation performance measure. This ensures that the contractor does not begin to deviate from the contract requirements.

- Credible:
    - Contract Value: The contract does not require a confidence level interval for accuracy and reliability.

- Accurate and Reliable: A comparison of the contract value above to the scale established in Chapter III indicates that the data is not accurate or reliable.

- Comparison:

  - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not monitor this criterion for the certificate revocation performance measure.

  - Accurate and Reliable: Since vendors do not monitor this measure, no comparison can be made between the vendor's value and the scale established in Chapter III.

The data collected from this performance measure is compared to the DON's random testing. If the contractor is reliable and accurate, the CRL will match the DON's revocation testing and will be within the timeframe required in the contract.

- Cost Effective:

  - Contract Value: The contract only requires the contractor to monitor this performance measure one way with no alternatives.

  - Cost-Effective: A comparison of the contract value above to the scale established in Chapter III demonstrates that this measure is not cost effective because no alternatives were provided.

- Comparison:
  - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not monitor this criterion for the certificate revocation performance measure.
  - Cost-Effective: Since vendors do not monitor this measure, no comparison can be made between the vendor's value and the scale established in Chapter III.

The contractor is contractually obligated to provide this data. The most efficient way of measuring this category is to have the contractor monitor themselves and be checked periodically by the DON.

- Comparable:
  - Have the conditions changed?:
    - Contract Value: The contract indicates that the contractor must provide monthly reports based on taking the same data the same way each time.
    - Comparable: A comparison the contract value above to the scale established in Chapter III demonstrates that the conditions for performing this measurement do not change.

- Comparison:
  - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not monitor this criterion for the certificate revocation performance measure.
  - Comparable: Since vendors do not monitor this measure, no comparison can be made between the vendor's value and the scale established in Chapter III.
- Has the definition for the variable changed?:
  - Contract Value: The contract requirements are outlined in the contract and should not change.
  - Comparable: Comparing the contract value above to the scale established in Chapter III demonstrates that the definition for the variable in this measurement does not change.
- Comparison:
  - Commercial Vendor: The data from Section B2 of Chapter III indicates that they do not monitor this criteria for the certificate revocation performance measure.
  - Comparable: Since vendors do not monitor this measure, no comparison can be made between the vendor's value and the scale established in Chapter III.

Since the contractor is responsible for keeping continuous records and providing monthly reports to the DON, a monthly analysis can be made to compare current revocation timeframes to past revocation timeframes. Unfortunately, initially, there is limited data available (either commercially or through government means) to use in evaluating this measure. This lack of data indicates that the DON will take longer to reach an effective revocation timeframe. However, this method also prevents the DON from reducing the revocation timeframe too much, and having to make further adjustments in the future.

With the rapid advances in technology this author believes that there will be software available to monitor the certificate revocation process automatically, and the DON's random testing will ultimately be phased out. Obviously if any software is used it will have to be fully tested by the DON prior to its deployment. This performance measure will become increasingly more important as the N/MCI contractor becomes fully deployed in the next two years, and the possibility of security breaches intensifies. The recommendations section below discusses these concerns further and will compare this performance measure to the limited commercial performance measures that are available.

b. Ability of One N/MCI User to Obtain a Certificate of Another N/MCI User

Description: Time required for users to successfully obtain, on the first attempt, the X.509 certificates from the N/MCI Public Key Infrastructure. [Ref. 2] The N/MCI performance measure to obtain a certificate is analyzed below using the analytical concepts from Chapter III. First the contract values will be provided, then the scale from the analytical concepts in Chapter III will be used to determine if the measurements meet

the standards. Finally, the data collected for this measure will be analyzed using the analytical concepts from Chapter III.

- Meaningful:
    - Contract Value: The contract indicates that the user certificates should be retrieved within 5 minutes (2 minutes for classified certificates).
    - Probability of Mission Success: Comparing the contract value above to the illustrative scale in Table 3-2, a value of 100% is obtained.
  - Comparison:
    - Commercial Vendors: The data from Section B2 of Chapter III indicates that user certificates are retrieved within 5 seconds to 5 minutes.
    - Probability of Mission Success: Comparing the commercial values above to the illustrative scale in Table 3-2, values of 100% and 100% are obtained.

This data illustrates that this performance measure is within commercial standards and a command's mission performance should be successful.

- Responsibility Related:
    - Qualifications:
        - Contract Value: The contract does not specify the qualifications of the person performing this measure.
        - Scale: Comparing the contract value above to the illustrative scale in Table 3-6, a value of 0 is obtained.
    - Comparison:
        - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not require any qualifications for the person performing this measure.
        - Scale: Comparing the commercial value above to the illustrative scale in Table 3-6, a value of 0 is obtained.
    - Incentive for data:
        - Contract Value: The contract indicates that the contractor will receive monetary incentives for performance values within contract requirements.
        - Scale: Comparing the contract value above to the illustrative scale in Table 3-7, a value of 100 is obtained.

- Comparison:
  - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not have to provide any incentive for performing this measure.
  - Scale: Comparing the commercial value above to the illustrative scale in Table 3-7, a value of 0 is obtained.
- Ability of person collecting data.
  - Contract Value: The contract does not specify the ability of the person performing this measure
  - Scale: Comparing the contract value above to the illustrative scale in Table 3-8, a value of 0 is obtained.
- Comparison:
  - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not require any qualifications for the person performing this measure.
  - Scale: Comparing the commercial value above to the scale in Table 3-8, a value of 0 is obtained.

This data illustrates that the contract does not require a person who is qualified to perform the measurement. It also indicates that the contractor will receive incentive pay for producing measurements that are within the contract requirements.

- Time Interval:
    - Contract Value: The contract indicates that the contractor must continuously collect the data for this performance measure, but only reports it monthly.
    - Timeliness: Comparing the contract value above to the illustrative scale in Tables 3-9 and 3-10, values of 5 for monitoring and 2 for reporting are obtained.
  - Comparison:
    - Commercial Vendors: The data from Section B2 of Chapter 3 indicates that they do not monitor this criteria for the user certificate retrieval performance measure.
    - Timeliness: Since vendors do not monitor this measure, no comparison can be made between the vendor's value and the scale established in Chapter III.

The DON has no intention of verifying that the contractor is performing this measure. Therefore, the DON will have to trust the contractor's results. Since the DON has no past contractual relationship with EDS this trust will take several months to develop. Monthly reports should provide sufficient coverage for this performance measure. This should ensure the contractor's systems are operating efficiently.

- Credible:
    - Contract Value: The contract does not require a confidence level interval for accuracy and reliability.
    - Accurate and Reliable: A comparison of the contract value above to the illustrative scale established in Chapter III indicates that the data is not accurate or reliable.
  - Comparison:
    - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not monitor this against the standard for the user certificate retrieval performance measure.
    - Accurate and Reliable: Since vendors do not monitor this measure, no comparison can be made between the vendor's value and the scale illustrative established in Chapter III.

The government has no plans to conduct any additional testing to verify the contractor's results. [Ref. 2] The DON will rely on the contractor's results and possibly customer feedback data for this performance measure. Therefore, with the current requirements, it is difficult to determine if the contractor is reliable and accurate.

- Cost Effective:
    - Contract Value: The contract requires the contractor to manually monitor this performance measure and does not provide any alternatives.
    - Cost-Effective: A comparison the contract value above to the illustrative scale established in Chapter III demonstrates that this measure is not cost effective because no alternatives were provided.
  - Comparison:
    - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not monitor this criterion for the user certificate retrieval performance measure.
    - Cost-Effective: Since vendors do not monitor this measure, no comparison can be made between the vendor's value and the illustrative scale established in Chapter III.

Based on the fact that the contractor is contractually obligated to provide this data, it is the author's opinion that the most efficient way of measuring this category is to have the contractor monitor themselves and be periodically checked by the DON. The DON should not invest in the resources to monitor this performance measure unless an inordinate amount of unsatisfactory customer complaints concerning this performance measure are received.

- Comparable:
    - Have the conditions changed?:
        - Contract Value: The contract requires the contractor to provide monthly reports based on taking the same data the same way each time.
        - Comparable: A comparison the contract value above to the illustrative scale established in Chapter III demonstrates that the conditions for performing this measurement do not change.
    - Comparison:
        - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not monitor this criteria for the certificate revocation performance measure.
        - Comparable: Since vendors do not monitor this measure no comparison can be made between the vendor's value and the illustrative scale established in Chapter III.
    - Has the definition for the variable changed?:
        - Contract Value: The contract requirements are outlined in the contract and should not change.
        - Comparable: A comparison of the contract value above to the illustrative scale established in Chapter III demonstrates

that the definition for the variable in this measurement does not change.

- Comparison:
  - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not monitor this criteria for the certificate revocation performance measure.
  - Comparable: Since vendors do not monitor this measure no comparison can be made between the vendor's value and the illustrative scale established in Chapter III.

Since the contractor is responsible for keeping continuous records and providing monthly reports to the DON, an analysis can be made using these reports. Unfortunately, initially, there is limited data available (either commercially or through government means) to use in evaluating this measure. This lack of data indicates that the DON will take longer to reach an effective timeframe for this measure. However, this method also prevents the DON from reducing the measure timeframe too much, and having to make further adjustments in the future.

This performance measure is a customer satisfaction issue as well as a security issue (the delay in getting a certificate could cause a delay in sending an encrypted message). The recommendations section below discusses this concern further.

c. Timeliness of User Registration for a DOD Certificate

Description: It measures the time from the submission of a user's request until a fully functional DOD PKI X.509 certificate is received by the user. [Ref. 2] The

N/MCI performance measure to obtain a certificate is analyzed below using the analytical concepts from Chapter III. First the contract values will be provided, then the scale from the analytical concepts in Chapter III will be used to determine if the measurements meet the standard. Finally, the data collected for this measure will be analyzed using the analytical concepts from Chapter III.

- Meaningful:
    - Contract Value: The contract requires that certificates should be created within 2 weeks (1 week for service level 3).
    - Probability of Mission Success: Comparing the contract value above to the scale in Table 3-3, a value of 0% is obtained.
  - Comparison:
    - Commercial Vendors: The data from Section B2 of Chapter III indicates that certificates are created within 5 minutes to 14 days.
    - Probability of Mission Success: Comparing the commercial values above to the illustrative scale in Table 3-3, values of 100% to 0% are obtained.

This data illustrates that this performance measure is not within commercial standards, and a command's mission performance may not be successful.

With the amount of DON members reporting to new commands everyday, this performance measure is critical to allowing a command to complete its mission in a timely manner. A member should be able to report to a new command and start operating almost immediately. Service levels one and two allow the contractor two weeks to register a new user. This amount of time seems excessive and may hinder a command's mission performance. Similarly, the one week for service level three could impact the mission performance as well.

- Responsibility Related:
    - Qualifications:
        - Contract Value: The contract does not specify the qualifications of the person performing this measure.
        - Scale: Comparing the contract value above to the illustrative scale in Table 3-6, a value of 0 is obtained.
    - Comparison:
        - Commercial Vendors: The data from Section B2 of Chapter 3 indicates that they do not require any qualifications for the person performing this measure.
        - Scale: Comparing the commercial value above to the illustrative scale in Table 3-6, a value of 0 is obtained.

- Incentive for data:
  - Contract Value: The contractor will receive monetary incentives for performance values within contract requirements.
  - Scale: Comparing the contract value above to the illustrative scale in Table 3-7, a value of 100 is obtained.
- Comparison:
  - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not have to provide any incentive for performing this measure.
  - Scale: Comparing the commercial value above to the illustrative scale in Table 3-7, a value of 0 is obtained.
- Ability of person collecting data.
  - Contract Value: The contract does not specify the ability of the person performing this measure
  - Scale: Comparing the contract value above to the illustrative scale in Table 3-8, a value of 0 is obtained.
- Comparison:
  - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not require any qualifications for the person performing this measure.

- Scale: Comparing the commercial value above to the illustrative scale in Table 3-8, a value of 0 is obtained.

This data illustrates that the contract does not require a person who is qualified to perform the measurement. It also indicates that the contractor will receive incentive pay for producing data that is within the contract requirements.

- Time Interval:
  - Contract Value: The contract indicates that the contractor must continuously collect the data for this performance measure, but only report, it monthly.
  - Timeliness: Comparing the contract value above to the illustrative scale in Tables 3-9 and 3-10, values of 5 for monitoring and 2 for reporting are obtained.
  - Comparison:
    - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not monitor this criteria for the certificate creation performance measure.
    - Timeliness: Comparing the vendor's value above to the illustrative scale in Tables 3-9 and 3-10, values of 0 for monitoring and 0 for reporting are obtained.

The DON has no intention of verifying that the contractor is performing this measure. Therefore, the DON will have to trust the contractor's results. Since the

DON has no past contractual relationship with EDS this trust will take several months to develop. Monthly reports should provide sufficient coverage for this performance measure. This should ensure the contractor's systems are operating efficiently.

- Credible:
    - Contract Value: The contract does not require a confidence level interval for accuracy and reliability.
    - Accurate and Reliable: A comparison of the contract value above to the illustrative scale established in Chapter III indicates that the data is not accurate or reliable.
  - Comparison:
    - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not monitor this against the standard for the certificate creation performance measure.
    - Accurate & Reliable: Since vendors do not monitor this measure, no comparison can be made between the vendor's value and the illustrative scale established in Chapter III.

The DON has no plans to conduct any additional testing to verify the contractor's results. The DON will rely on the contractor's results and possibly customer feedback data for this performance measure. Therefore, with the current requirements, it is difficult to determine if the contractor is reliable and accurate.

- Cost Effective:
    - Contract Value: The contract requires the contractor to manually monitor this performance measure one way with no alternatives.
    - Cost-Effective: A comparison the contract value above to the illustrative scale established in Chapter III demonstrates that this measure is not cost effective because no alternatives were provided.
  - Comparison:
    - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not monitor this criterion for the certificate creation performance measure.
    - Cost-Effective: Since vendors do not monitor this measure, no comparison can be made between the vendor's value and the illustrative scale established in Chapter III.

Based on the fact that the contractor is contractually obligated to provide this data, it is the author's opinion that the most efficient way of measuring this category is to have the contractor monitor themselves and be periodically checked by the DON. The DON should not invest in the resources to monitor this performance measure unless an inordinate amount of unsatisfactory customer complaints concerning this performance measure are received.

- Comparable:
    - Have the conditions changed?:
        - Contract Value: The contract indicates that the contractor must provide monthly reports based on taking the same data the same way each time.
        - Comparable: A comparison of the contract value above to the illustrative scale established in Chapter III demonstrates that the conditions for performing this measurement do not change.
    - Comparison:
        - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not monitor this against the standard for the certificate revocation performance measure.
        - Comparable: Since vendors do not monitor this measure no comparison can be made between the vendor's value and the illustrative scale established in Chapter III.
    - Has the definition for the variable changed?:
        - Contract Value: The contract requirements are outlined in the contract and should not change.

- Comparable: A comparison of the contract value above to the illustrative scale established in Chapter III demonstrates that the definition for the variable in this measurement does not change.

- Comparison:

  - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not monitor this criterion for the certificate revocation performance measure.

  - Comparable: Since vendors do not monitor this measure no comparison can be made between the vendor's value and the illustrative scale established in Chapter III.

Since the contractor is responsible for keeping continuous records and providing monthly reports to the DON, an analysis can be made using these reports. Unfortunately, initially, there is limited data available (either commercially or through government means) to use in evaluating this measure. This lack of data indicates that the DON will take longer to reach an effective timeframe for this measure. However, this method also prevents the DON from reducing the measure timeframe too much, and having to make further adjustments in the future.

This performance measure is more of a customer satisfaction issue rather than any type of security issue, especially with the need for transferring service members in a timely manner. The recommendations section below discusses this concern further.

d. Interoperability

Description: It measures the degree of interoperability and the level of seamless interface both internally within the N/MCI and externally, among non-N/MCI commands. [Ref. 2] As of the writing of this thesis, the contractor has not developed an interoperability test plan or the procedures that support this particular service, as required in the N/MCI contract. The N/MCI interoperability performance measure is analyzed below using the analytical concepts from Chapter III. First the contract values will be provided, then the scale from the analytical concepts in Chapter III will be used to determine if the measurements meets the standard. Finally, the data collected for this measure will be analyzed using the characteristics from Chapter III.

- Meaningful:
    - Interoperability between networks:
        - Contract Value: The contract does not specify a requirement based on the type of network with which the interoperability problems occur.
        - Probability of Mission Success: Comparing the contract value above to the illustrative scale in Table 3-4, a value cannot be obtained.
    - Comparison:
        - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not monitor this criterion for the interoperability performance measure.

- Probability of Mission Success: Comparing the vendor's value above to the illustrative scale in Table 3-4, a value cannot be obtained.

- System down-time due to interoperability:
  - Contract Value: The contract indicates that interoperability issues should be corrected within one day (4 hours for service level 3).
  - Probability of Mission Success: Comparing the contract value above to the illustrative scale in Table 3-5, a value of 75% is obtained.

- Comparison:
  - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not monitor this criteria for the interoperability performance measure.
  - Probability of Mission Success: Comparing the vendor's value above to the illustrative scale in Table 3-5, a value cannot be obtained.

This data indicates this measure is relevant to the DON's mission and their goal of eliminating interoperability problems between commands within the DON. This performance measure will also provide data on possible problems the DON may encounter when trying to communicate securely with other government agencies.

- Responsibility Related:
    - Qualifications:
        - Contract Value: The contract does not specify the qualifications of the person performing this measure.
        - Scale: Comparing the contract value above to the illustrative scale in Table 3-6, a value of 0 is obtained.
    - Comparison:
        - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not require any qualifications for the person performing this measure.
        - Scale: Comparing the commercial value above to the illustrative scale in Table 3-6, a value of 0 is obtained.
    - Incentive for data:
        - Contract Value: The contract indicates that the contractor will receive monetary incentives for performance values within contract requirements.
        - Scale: Comparing the contract value above to the illustrative scale in Table 3-7, a value of 100 is obtained.

- Comparison:
  - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not have to provide any incentive for performing this measure.
  - Scale: Comparing the commercial value above to the illustrative scale in Table 3-7, a value of 0 is obtained.
- Ability of person collecting data.
  - Contract Value: The contract does not specify the ability of the person performing this measure
  - Scale: Comparing the contract value above to the illustrative scale in Table 3-8, a value of 0 is obtained.
- Comparison:
  - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not require any qualifications for the person performing this measure.
- Scale: Comparing the commercial value above to the illustrative scale in Table 3-8, a value of 0 is obtained.

This data indicates that the contract does not require a person who is qualified to perform the measurement. It also indicates that the contractor will receive incentive pay for producing data that is within the contract requirements.

- Time Interval:
    - Contract Value: The contract indicates that the contractor must continuously collect the data for this performance measure, but only report it monthly.
    - Timeliness: Comparing the contract value above to the illustrative scale in Tables 3-9 and 3-10, values of 5 for monitoring and 2 for reporting are obtained.
  - Comparison:
    - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not monitor this criterion for the interoperability performance measure.
    - Timeliness: Comparing the vendor's value above to the illustrative scale in Tables 3-9 and 3-10, values of 0 for monitoring and 0 for reporting are obtained.

The DON has no intention of verifying that the contractor is performing this measure. [Ref. 28] Therefore, the DON will have to trust the contractor's results. Since the DON has no past contractual relationship with EDS this trust will take several months to develop. The reports should provide sufficient coverage for this performance measure. This should ensure the contractor's systems are operating efficiently.

- Credible:
    - Contract Value: The contract does not require a confidence level interval for accuracy and reliability.
    - Accurate and Reliable: A comparison of the contract value above to the illustrative scale established in Chapter III indicates that the data is not accurate or reliable.
  - Comparison:
    - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not monitor this against the standard for the interoperability performance measure.
    - Accurate and Reliable: Since vendors do not monitor this measure, no comparison can be made between the vendor's value and the illustrative scale established in Chapter III.

The DON has no plans to conduct any additional testing to verify the contractor's results. The DON will rely on the contractor's results and possibly customer feedback data for this performance measure. [Ref. 2] Therefore, with the current contract requirements, the only way the DON will determine if the contractor is reliable and accurate is through customer complaints.

- Cost Effective:
    - Contract Value: The contract requires the contractor to manually monitor this performance measure one way with no alternatives.
    - Cost-Effective: A comparison of the contract value above to the illustrative scale established in Chapter III demonstrates that this measure is not cost effective because no alternatives were provided.
  - Comparison:
    - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not monitor this criterion for the interoperability performance measure.
    - Cost-Effective: Since vendors do not monitor this measure, no comparison can be made between the vendor's value and the illustrative scale established in Chapter III.

Based on the fact that the contractor is contractually obligated to provide this data, it is the author's opinion that the most efficient way of measuring this category is to have the contractor monitor themselves and be periodically checked by the DON. The DON should not invest in the resources to monitor this performance measure unless an inordinate amount of unsatisfactory customer complaints concerning this performance measure are received.

- Comparable:
    - Have the conditions changed?:
        - Contract Value: The contract requires the contractor to provide monthly reports so the DON can compare them for trends in the contractor's performance.
        - Comparable: A comparison the contract value above to the illustrative scale established in Chapter III demonstrates that the conditions for performing this measurement do not change.
    - Comparison:
        - Commercial Vendors: The data from Section B2 of Chapter III indicates that they do not monitor this criterion for the interoperability performance measure.
        - Comparable: Since vendors do not monitor this measure, no comparison can be made between the vendor's value and the illustrative scale established in Chapter III.
    - Has the definition for the variable changed?:
        - Contract Value: The contract requirements are outlined in the contract and should not change.
        - Comparable: A comparison the contract value above to the illustrative scale established in Chapter III demonstrates

that the definition for the variable in this measurement does not change.

- Comparison:
  - Commercial Vendor: The data from Section B2 of Chapter III indicates that they do not monitor this criteria for the certificate revocation performance measure.
  - Comparable: Since vendors do not monitor this measure no comparison can be made between the vendor's value and the illustrative scale established in Chapter III.

Since the contractor is responsible for keeping continuous records and providing monthly reports to the DON, an analysis can be made using these reports. Unfortunately, initially, there is limited data available (either commercially or through government means) to use in evaluating this measure. This lack of data indicates that the DON will take longer to reach an effective timeframe for this measure. However, this method also prevents the DON from reducing the measure timeframe too much, and having to make further adjustments in the future.

This performance measure is a customer satisfaction issue as well as a security issue, (if important data is not available, it can be a security issue) especially with the timeliness of correcting interoperability issues. The recommendations section below discusses this interoperability issue further.

4. N/MCI Performance Measures Recommendations

a. Certificate Revocation

The contractor must follow the Department of Defense's PKI specifications as specified in the contract requirements. [Ref. 2] Currently, the contract requirements specify CRLs, but an alternative method for invalidating certificates (the on-line certificate verification process) is becoming popular. The problems associated with revocation are a rather new area of research, and on-line validation is even newer. On-line verification is being promoted as the more reliable and quicker answer to the revocation problem, however, this type of technology has never been proven on such a large scale enterprise as the DON. [Ref. 14] One advantage of on-line verification, over CRLs is the speed of retrieving up-to-date verification. The disadvantage of both on-lin verification and CRLs is the dependency on the network traffic. [Ref. 37]

The contract only specifies a requirement for the contractor to provide the certificate authority with the revocation notification. It does not indicate the timeliness of transmitting CRLs. It is recommended that the contractor adhere to one of the pilot program's standard of sending out or downloading a new CRL every four hours, and sending out a Delta-CRL every ten minutes. [Ref. 35]

When comparing the commercial performance measures for certificate revocation with the N/MCI contract performance measures, this thesis will assume that the authors of the N/MCI contract intended that the time restrictions include the distribution of the CRLs.

By comparing the certificate revocation time advertised by commercial PKI businesses to the time indicated in the N/MCI contract, it is clear that the contract requirement specifies an adequate time for DOD Class 3 PKI certificate revocation.

Since CRLs have been proven to be a secure and trustworthily form of certificate revocation, it is recommended that the N/MCI contractor continue using CRLs until DISA/NSA determine that the DOD Class 3 PKI can support on-line verification. [Ref. 19] Once on-line verification is fully established for DOD, it is recommended the N/MCI contractor switch their process to this scheme, and the N/MCI performance measure be reduced to reflect commercial performance measures. Based on the research done in this thesis, this change would reduce the performance measure down to a maximum of two minutes for a revocation to take place. [Ref. 14] Prior to changing over to on-line verification the government can use data collected by the green team to adjust the PKI revocation contract requirements as necessary.

Due to the extreme importance of having certificate-based trust within the N/MCI, this area of the contract must be strictly monitored for compliance. Without complete and timely management of revocations, the entire Department of the Navy would have less trust of the certificates they encounter on a day-to-day basis.

b. Ability of One NMCI User to Obtain a Certificate of Another NMCI User

The performance measure for this category in the N/MCI contract is aligned with the commercial industry. Receiving a user's public key within the contract specification of five minutes should be adequate considering the number of DON users. However, with the advancement in PKI technology, it is possilbe that this value will be

decreased in the future. By that time, the N/MCI contractor should have in place an extensive network of key directories that will provide a user's public key almost instantaneously.

There is concern about how the contractor is going to collect this data on obtaining certificates and prove to the government that it is correct and accurate data. The contractor's incentive pay is based on these findings, so it is recommended that there be some form of government monitoring of this performance measure. It is recommended that monitoring be completed at random intervals and at random commands, where actual timing is done on the acquiring of a user's public key. At the very least, this should be a section included in the customer satisfaction form, so that users can provide feedback on their experiences.

c. Timeliness of User Registration for a DOD Public Key

The contract required time frame for certificate creation, which is one week for 85 percent of the certificates, and two weeks for 100 percent of the certificates, is extremely high when compared to the commercial industry. The contractual values were developed over two years ago when PKI was fairly new in the DOD and there was no data available on the length of time required for certificate creation within a large PKI. [Ref. 27] Today's commercial PKI businesses proclaim timelines in a scale of minutes, which is much less than or much faster than the N/MCI performance measure value. It is understandable that the DON has to go through a more rigorous application interview. However, if commands are to maintain a high level of mission readiness it is recommended that this performance measure be reduced to one day.

The current N/MCI performance measure could lead to a possible loss of productivity. This loss is most prevalent when a service member transfers to a new command and may have to wait two weeks until they can log onto a computer and be productive. Service members who are temporarily assigned to other commands could also have problems communicating securely within a reasonable timeframe. Finally, service members work seven days a week, and the contract does not specifically require providing certificates on the weekend. It is recommended that this be clarified so this issue does not become a problem in the future.

These N/MCI performance measures were developed with the shear size of the DON in mind and consideration for how the N/MCI contractor would process all of these members. However, the contractor is being phased in, and the issuance of these certificates is being phased in as well. Also, it is likely that the contractor will have more than one issuing agency throughout the DON. Even with these issues, the above recommendation to reduce the time it takes to create a certificate is still valid.

The government is not monitoring this performance measure and will rely almost entirely on the data that the contractor supplies. Since the contractor receives incentive pay to maintain this performance measure, it is recommended that random checks at various CA/RA/LRAs be completed on a monthly basis to ensure that the contractor is, at the very least, meeting the contract requirements. These random checks will provide the DON sufficient data to ensure the level of service does not degrade over the five year contract length. Due to the possibility that a vast amount of productivity could be lost to the registration process, the author believes that this will be the number

one customer satisfaction issue. It is recommended that this be part of the customer satisfaction form, at the very least.

d. Interoperability

The public key infrastructure outlined in the Navy Marine Corps Intranet contract is not the first government PKI program. The government has established several PKI pilot programs in different agencies throughout the DOD. The government has recognized the need to have these PKIs be interoperable. With that in consideration, the Federal PKI (FPKI) agency has been working with Entrust Technologies to develop the Federal Bridge Certification Authority (FBCA). The FBCA and FPKI CAs are networked together and linked to the Canadian Federal Government's Entrust PKI to create a trusted test environment for the validation of digital certificates and exchange of secure information between the participants. [Ref. 18] See Figure 4-1 The FBCA acts as a trusted third party to ensure that, when a user needs to accept a PKI certificate from another body, the certificate can be trusted regardless of which CA issued it.

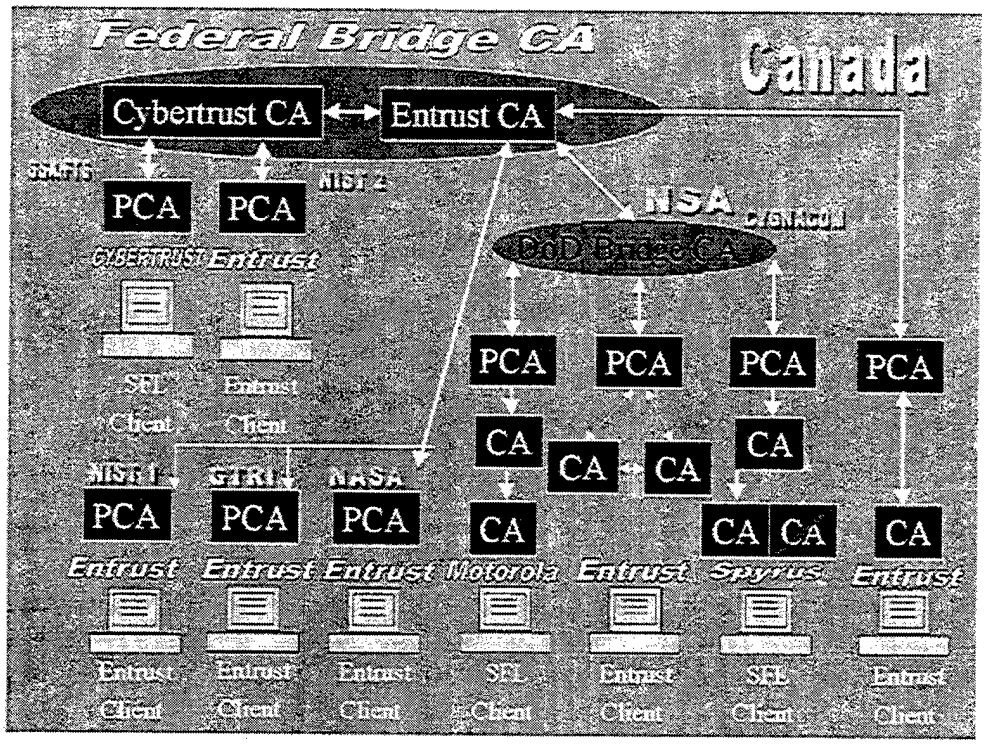


Figure 3-1. FBCA. [From Ref. 18]

The DON interoperates with a large number of other public key infrastructures including Allies, commercial contractors and other DOD agencies. Since the DOD PKI is based primarily on using commercial standards, it will allow interoperability with most US entities and the DON. However, this may not be acceptable if the DON has to interoperate with non-US entities (e.g., Allies and Coalition partners). [Ref. 19] Therefore, the author recommends that the N/MCI contractor become a member in the FBCA so that the above possible interoperability issues can be eliminated.

One interoperability issue that has not been discussed is the requirement that all DOD PKIs use the Netscape Communicator 4.7 browser. This browser was selected by the DOD as the standard certificate based application for DOD certificates.

However, the N/MCI contract requires the contractor to supply each computer station with Microsoft's Internet Explorer browser. This interoperability issue will need to be resolved. One resolution is to install Netscape on each N/MCI computer.

5. Cost Analysis of the Recommended Changes

A complete cost analysis on any recommended changes is beyond the scope of this thesis. However, a brief look at possible contract increases for each of the recommend changes follows. Note: This is by no means a conclusive analysis.

a. Certificate Revocation

After the government validates the process of on-line certificate revocation and the contract is modified to reflect this technology, the changes should not result in an increase in the government's costs. The contract requires the contractor to adapt their current technology to industry changes. [Ref. 2] On-line verification is a technology that could be well established in the commercial industry by the time the government decides to implement it, so the measurements should be modified to reflect industry standards without penalty to the DON.

b. Ability of One NMCI User to Obtain a Certificate of Another NMCI User

The random government monitoring of this measure could be done at a very minimal cost. This random test could be done by the SPAWAR's green team at the same time they test the certificate revocation. The agency responsible for monitoring customer service could also add a response time question on surveys to gather the data. Finally, with today's technology, this process could be remotely monitored by a computer application that issues monthly reports to the N/MCI contracting officer. This cost would only be for initial application setup and some monitoring.

c. Timeliness of User Registration for a DOD Public Key

Reducing the timeline of registration to one day for 85% completion and two days for 100% completion should not be a cost to the government. The contract was written when PKI's were first starting to become a viable e-commerce security program, and the contractual time frame was adequate at that time. However, PKI technology has developed tremendously, and the above recommendation should be the contractual standard. If there are any costs incurred for this change, the government is sure to recoup these costs through the decrease in production losses.

Monitoring of this performance measure could involve some substantial costs if it were to be physically monitored by someone. However, this is a measure that can be monitored through customer satisfaction surveys and would not be any additional cost to the government.

d. Interoperability

Decreasing the time of having one system interoperate with another system down to four hours for all service levels will probably add costs to the N/MCI contract. The contractor could incur additional costs trying to maintain that level of service. However, this is only a temporary situation that should only last at most the first two years.

It is the author's opinion that the public key infrastructure portion of the contract have strong measures at whatever cost to the government, to insure that possible espionage does not occur. Any penetration into our defense systems could cost the government loss of infrastructure and possibly the cost of human life.

C. TRANSITION TO N/MCI

1. Past Beliefs

As stated in Appendix A, throughout history, governments have sent messages securely between commands using one-key encryption. This method has worked efficiently for years, and because a majority of this was accomplished by only a select few, most service members never dealt with possible security issues. Unfortunately, technology has forced security requirements down upon the entire fleet.

This new technology impact is not only felt in security issues. With the implementation of the N/MCI contract, the DON will have to change the way it procures and manages information technology. Commands that previously were responsible for ensuring that their technology was as current as the rest of the fleet will no longer be responsible for this. The N/MCI contractor will have the responsibility of keeping commands' information technology current. Unfortunately, all the commands' IT concerns are not erased with the implementation of the N/MCI. With this contract come new problems and issues that are discussed in the next section.

2. Future Concerns

The current way the DON operates is in state of major reconstruction. Technology has driven our old methods of conducting business out the door and service members are going to have to adapt to this new technology. Public key infrastructure will demand that our systems become more secure. This means that just logging on to our system will take extra effort. The government has mandated that every DON member be issued a Class 3 level (Medium Assurance) certificate by the end of October

2001. To support this, Smart Cards will be issued. These will not only be a service member's personnel identification card, but will also be required to access DON systems by inserting it in a Smart Card reader.

The majority of the service members should have no problem adapting to this new way of accessing their systems. It is likely that the problems with these technology changes revolve mainly around senior civilian employees (currently 50 percent of government employees are within two years of retirement). [Ref. 7] Some of these individuals might require a longer learning curve to adapt to this technology, and some may protest against these changes.

Parallel with these security changes, the DON is going through other changes with the new N/MCI. Commands will have to adapt to letting others decide which hardware, software, and infrastructure they should have. Senior commanders may have a hard time giving up this control, while others may invite these changes so that they do not have to deal with the decisions. One impact that can be foreseen is a command demanding more computers than what is outlined in the N/MCI contract. This issue is likely to be based on a difference of opinion, and the deciding vote will probably be the N/MCI contracting officer.

Another future concern is that commands may operate separate computers that are not controlled under the N/MCI contract. This would allow the command to run software that the N/MCI contractor may not provide. These non-standard computers could cause interoperability problems and decrease production – the very problems that the N/MCI was implemented to correct. This could also create double the work for command

administrative personnel and create possible inconsistencies between commands. Also, funding for N/MCI is given to commands so that information technology costs can be tracked for each command. If commands spend funds allotted for other programs on non-N/MCI technology, it will contribute to an inaccurate accounting of how much the DON is actually spending on information technology.

Obviously there are several issues that will surface during this tremendous transformation. Hopefully, the government is analyzing the problems that occur as the N/MCI is implemented. Additionally, the DON needs to communicate these issues with the entire fleet prior to full implementation, so that commands can be proactive regarding the problems, vice reactive.

D. PERFORMANCE MEASURE CONTROLS

As discussed in the above sections the government is giving the N/MCI contractor considerable leeway in the monitoring of the PKI performance measures. Specifically, certificate revocation is the only PKI performance measure that is being monitored by the DON in an attempt to verify that the N/MCI contractor is performing correctly. The DON is paying the contractor an incentive fee for all the PKI performance measures where they provide satisfactory service. Unfortunately, the DON is basing their satisfactory service on the reports provided by the N/MCI contractor. [Ref. 2] The above issues are further discussed in the sections below.

1. Green Team Monitoring

The only performance measure that the government is required to verify is the timely revocation of a certificate. The other three performance measures are conducted

by the N/MCI contractor and they submit unverified monthly reports. A green team has been established at the Space and Naval Warfare Systems Command (SPAWAR) to conduct tests necessary to judge compliance of the certificate revocation performance measure. [Ref. 28] Unlike red teams, who conduct unannounced vulnerability testing using cutting edge hacker technology, green teams are designed for the purpose of verifying the compliance of a specific area, and they make their presence fully known to the contractor. [Ref. 28]

2. Performance Incentives

The N/MCI contract was awarded to Electronic Data Systems Corporation (EDS) of Plano, Texas for $6,938,817,954. There is a guaranteed five year basic period plus the three year option period. [Ref. 26] EDS has the opportunity to increase this amount by meeting certain performance incentives, outlined in the contract. The major incentive is through seat service performance, which can range from $25 to $100 per quarter, per seat, depending on the rating of their service. Incentives will also be given for information assurance, small business participation, and achievement of full operational capability. For the fiscal year 2001, the incentives could add up to $38.8 million. [Ref. 16]

3. Control of Revocation Incentives

If the DON concludes that the contractor is not adhering to the contract requirements for the revocation of certificates, the DON may have to modify the contract to increase inspections and hold back incentive pay. This category is far too important to national security to allow for any slippage in the revocation time. If the revocation

processes were to fail, the costs could be far greater than money, as in, loss of life, or threat to the national security.

Finally, the contractor is responsible for keeping continuous records and providing monthly reports to the DON. A monthly analysis can be made that compares current revocation timeframes to past revocation timeframes. This should allow the DON the ability to modify the N/MCI contract if the situation warrants. Additionally, the DON plans on conducting customer surveys that should provide feedback on how the contractor is performing thus supplying the DON with another control measure.

THIS PAGE INTENTIONALLY LEFT BLANK

V. IMPACTS OF N/MCI

As discussed in Chapter II the N/MCI contract is the largest outsourcing contract the DON has undertaken. Because of the size of the contract, several areas of the DON are affected. The following provides the reader with an idea of how the N/MCI is affecting the DON.

A. COST OF CONTRACT

This thesis analyzes the performance measures for the PKI service level agreement. The ability to meet these predetermined agreements will determine the amount of incentives the contractor will receive. The tangible and intangible costs for the contract are analyzed below.

1. Cost of IT Pre N/MCI Award

Prior to the implementation of the N/MCI (N/MCI will not be fully functional until FY 2003), the Navy and Marine Corps funded their IT through their normal Operations and Maintenance funds. These costs were never tracked accurately. This is due to the fact that commands used other mission funding to acquire their IT infrastructure and keep up with the current technology. [Ref. 16] Table 5-1 shows the Department of the Navy's estimated IT costs for FY 1996 through FY 2000 (Pre N/MCI):

Table 5-1. DON Information Technology Costs. [From Ref. 16]

FY 1996	FY 1997	FY 1998	FY 1999	FY 2000
$2,153	$2,294	$2,880	$3,573	$3,632

(in millions of dollars)

As seen from the above table, the estimated IT costs increased 59% over the last five years. During the same period, the DON has only increased IT funding a mere 10%. [Ref. 16] This considerable difference is attributed to the DON inaccurately forecasting IT costs. However, their forecasts were distorted because commands improperly tracked their IT costs. Presently, the costs have increased far beyond commands' budgets. [Ref. 16] All of these reasons support the implementation of an enterprise-wide, common IT infrastructure, such as the N/MCI, for the entire DON.

2. N/MCI Estimated Budget

Although exact costs (fixed costs plus incentives) for the N/MCI have not been determined - the contract was awarded in October 2000 - the DON did a complete estimate prior to award. Their estimate of $1.5 billion annually for all IT requirements was additionally verified by the comparable bids they received from the commercial solicitations. [Ref. 16]

The estimated N/MCI budget for FY 2001 through FY 2005 is outlined in Table 5-2 below:

Table 5-2. N/MCI Estimated Budget. [From Ref. 16]

FY 2001	FY 2002	FY 2003	FY 2004	FY 2005
$256.1*	$1,054.3*	$1,463.4	$1,463.4	$1,463.4

(in millions of dollars)

(*Values are low because N/MCI will not be fully implemented until the end of FY 2002, and do not include the Non-N/MCI IT costs)

The DON plans on distributing the required funding to each command, based on its individual IT needs. This will permit the command's IT budget to reflect its entire operational IT costs. The DON determines that the N/MCI will save the government $3.5

billion over the five-year contract. [Ref. 17] These savings give some justification for the DON's decision to outsource their entire information technology infrastructure.

B. CIVILIAN DON EMPLOYEES

The DON has identified 1,900 personnel whose jobs are affected by the implementation of the N/MCI. The contract requires EDS to allow these people the opportunity to be the first to apply for positions under the N/MCI contract. Presently all but 326 people have been given positions performing different functions within EDS. EDS is also paying a $25,000 signing bonus and a 30% pay increase to anyone joining their company with guaranteed employment for three years. [Ref. 17] Since there are so many displaced personnel from the DON it is the author's opinion that personnel pose a possible security threat. The displaced personnel are the same individuals who will manage the DON systems, for the N/MCI contractor, and have ample opportunity to inflict possible security breaches.

C. MARINE CORPS

Unlike the Navy, the Marine Corps has created a central control network and a standard infrastructure throughout its commands. The Marine Corps combined their garrison and tactical command, communications, computers, and intelligence systems almost 10 years ago. The garrison represents the Marine's nondeployable assets and their tactical resources can be compared to the Navy's deployable IT-21 ship-based IT assets. Under the N/MCI, EDS will only be responsible for the garrison portion. The Marine Corps is concerned that the N/MCI contractor will not manage the garrison's IT equipment correctly. Specifically, they are concerned with a possible mismatch between the garrison's equipment and the tactical resources. [Ref. 17] EDS is under rigorous

scrutiny by the Marine Corps to provide a seamless connection between the garrison and the tactical networks.

VI. CONCLUSIONS

A. THESIS SUMMARY

Chapter II of this thesis provided the reader with an overview of the Navy Marine Corps Intranet contract. It analyzed how the N/MCI contract was created and the shortened path it took to be awarded. It also discussed the roles of other agencies and how they operate within the N/MCI. A further review of the entire N/MCI contract can be done by going to the Navy Program Management Office's web site: https://nmci.spawar.navy.mil/.

Chapter III analyzed performance measures, criterion, and standards. This chapter's content focused on the necessary concepts for understanding measures, criterion, and thus standards.

Chapter IV analyzed the PKI performance measure requirements in the N/MCI contract. In this chapter, the thesis compared the N/MCI contract requirements to the commercial PKI industry performance measures using the characteristics discussed in Chapter III.

Chapter V discussed the specific areas of the DON that are covered by the N/MCI, and the cost impact of the N/MCI.

Appendix A provides a review of the DOD Public Key Infrastructure and the related cryptographic PKI issues. If the reader is unfamiliar with PKI issues, some of the referenced PKI books in the appendix can be referenced.

PKI technology has been around in one form or another for several years, however, the need for PKI has only recently surfaced. This rise in necessity for PKIs can

be attributed to the rise in e-commerce concerns. In the near future, to properly secure transmissions over the Internet, the transparent use of a PKI will become part of everyone's life. As indicated in chapter II, a PKI is a required security component for the new Navy Marine Corps Intranet and is used by the Department of the Navy personnel.

B. PEFORMANCE MEASURES

As discussed in Chapter III and IV of this thesis, the commercial industry is not monitoring performance measures in the same way that the DON wants EDS to. This made the comparison between commercial performance measures and contract requirements very difficult. Additionally, PKI is in its infancy, in terms of usage, which has contributed to the lack of performance measures for comparison. Commercial implementations of PKI have only occurred in smaller companies, which complicates the comparison with a DON-wide implementation. However, enough data was collected to make an intelligent evaluation of the N/MCI PKI contract requirements. The indicated performance measures were, in general, a good start for this contract. Still, as discussed in this thesis, there is room for improvement.

The importance of the DON commands communicating securely through the Internet is something that should not be taken lightly. The monitoring of these performance measures is necessary to provide a sufficient degree of security and hopefully keep our members out of harms way.

C. RECOMMENDATIONS FOR FUTURE RESEARCH

During the writing of this thesis, it was instantly obvious that there was very little data, from either commercial vendors or other government PKI programs, for which to

conduct a very detailed comparison with the N/MCI requirements. With that in mind, it is strongly recommended that a similar PKI performance measure thesis be conducted after the first year of the implementation of the N/MCI contract. This should provide sufficient time for the contractor to collect actual DON data from their systems. Furthermore, the commercial industry is rapidly adapting to PKI for e-commerce, and hopefully, within a year, there will be an abundance of commercial data to make a more detailed comparison.

There is also a concern that the N/MCI contractor will install the PKI technology throughout the DON without giving the members sufficient training on how to use the PKI to communicate securely over the Internet. It is recommended that a thesis be done on what, if any, PKI training members are receiving and if it is sufficient to ensure that the DON is not creating a bigger security threat with the implementation of N/MCI.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A: PUBLIC KEY CRYPTOGRAPHY AND PUBLIC KEY INFRASTRUCTURE

This appendix presents an overview of Public Key Cryptography and Public Key Infrastructure. This overview allows the reader to understand the basis of performance measures. A more detailed understanding of these mechanisms can be acquired from the list of referenced material.

A. SYMMETRIC KEY CRYPTOGRAPHY: ONE KEY

Symmetric key encryption, (commonly known as conventional key encryption or session key encryption), has been used in the military for almost as long as there has been a military. Conventional encryption is based on the sender and the receiver having identical keys. This is why it is called symmetric cryptography. With conventional key cryptography a message is encrypted with a key and the receiver of the encrypted message uses the same key to decrypt it back into the original message. [Figure A-1]

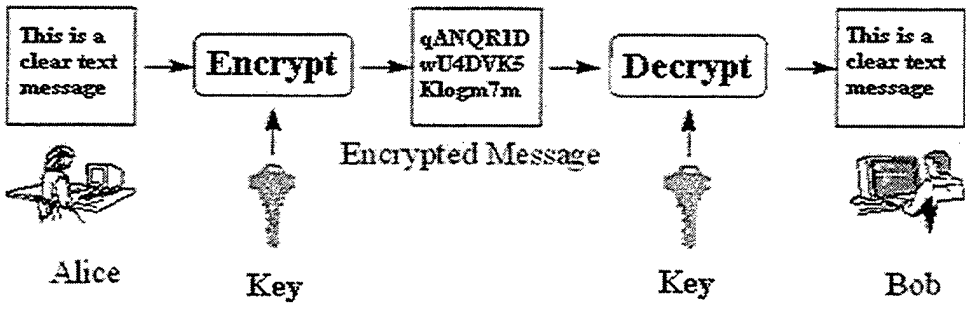


Figure A-1. Conventional Key System. [After Ref. 7]

Conventional key encryption has worked very successfully in the past. However, with the increased use of the Internet, intranets, and extranets to transmit unclassified-

but-sensitive messages, the distribution of keys - which is major drawback of conventional cryptography - is becoming significantly more difficult. Similarly, if there are multiple receivers of a message, each receiver will need a copy of the session key used to encrypt the message. Furthermore, if each participant wants to transmit an encrypted message of his own, each receiver would need a copy the encryption key. In a real world scenario, the number of individual session keys grows out of control and can be summarized in a mathematical equation:

n * (n-1)/2 keys are required for n users. [From Ref. 6]

There is also a very real concern regarding the security of how receivers and senders obtain the keys. This has often been accomplished through sneaker-mail (i.e. the transfer of a key by hand-delivery), which allows for a weak link in the security structure. Further, as indicated by the formula above, it becomes infeasible to hand deliver symmetric keys to a large number of users. This factor limits the scalability of a conventional key system. It also limits performance due to the time consuming hand-delivery process.

In addition to these problems of key distribution and management, conventional cryptography cannot support a true digital signature. The next section illustrates how public key cryptography can address conventional key distribution and management problems as well as true digital signatures.

B. PUBLIC KEY CRYPTOGRAPHY: TWO KEYS

Public key cryptology was developed by Whitfield Diffie and Professor Martin Hellman at Stanford University in 1976. [Ref. 8] Ronald Rivest, Adi Shamir, and

Leonard Adleman, all professors at the Massachusetts Institute of Technology, devised a set of algorithms that helped popularize Public Key Cryptography. Their system is known as RSA, after their last names. This section discusses public key encryption, its uses, and its advantages over conventional encryption.

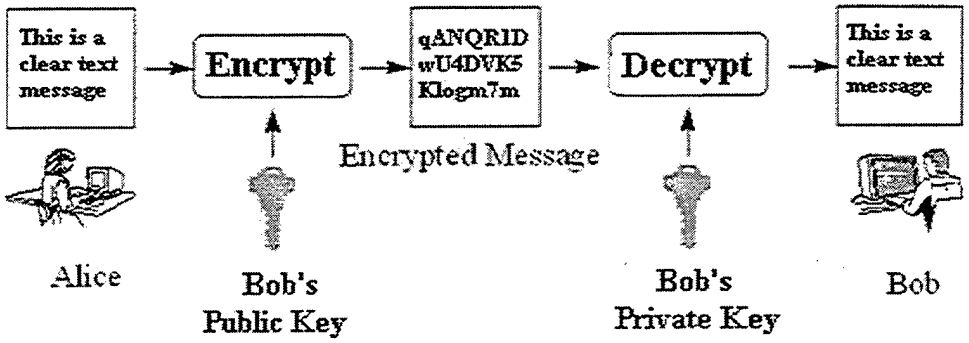


Figure A-2. Public Key System. [After Ref. 11]

Public key cryptography uses two mathematically releated keys, a public key and a private key. These keys are not identical, as in conventional encryption, and that is why public key cryptography is called asymmetric key cryptography. [Figure A-2] Each user is assigned a public key and a private key that are linked solely to that individual. An underlying principle of public key cryptography is that a user's private key must always be kept secure.

The counterpart to the private key is the public key. This key is made available to the public. Public key issues are discussed in the Public Key Infrastructure section below (Section C). The following sub-sections show how public key systems support the security services of confidentiality and digital signatures.

1. Confidentiality

Confidential is defined in Webster's Dictionary as "containing information whose unauthorized disclosure could be prejudicial to the national interest". The goal is to keep data secret by preventing unauthorized individuals from reading it. A message sent in plain text format can be read by an eavesdropper. Since public key encryption is notoriously slow at encrypting data, a hybrid technique that uses both conventional and public key cryptography is commonly used.

When a message is encrypted using this technique, the following steps are performed:

Step 1: A conventional key is randomly generated.

Step 2: The message is encrypted with the conventional key.

Step 3: The conventional key is encrypted with the receiver's public key.

Step 4: The encrypted message and encrypted conventional key are sent to the receiver.

The receiver retrieves the original message by performing the following steps:

Step 1: Uses his or her private key to decrypt the conventional key.

Step 2: Uses the conventional key to decrypt the original plain text message.

2. Digital Signature

A digital signature of a message uses cryptographic techniques to provide the same properties as a handwritten signature. Digital signatures are now legally binding as

a result of recent Federal legislation. A digital signature of a message is created using the following steps:

Step 1: A hash value of the message is computed - (A hash value is a very complicated checksum that satisfies the property that if the hash of a message M1 is equal to X, it is computationally infeasible to find another message M2, such that the hash of M2 is equal to X).

Step 2: The hash value is encrypted with the sender's private key. The encrypted hash value is the digital signature of the message.

The signature verification process of a digital signature uses the following steps:

Step 1: A hash value of the received message is computed.

Step 2: The digital signature (the private key encrypted hash value) is decrypted using the sender's public key.

Step 3: If the hash value in the first step is the same as the hash value in the second step, the signature is valid and establishes message authenticity and message integrity. [Figure A-3]

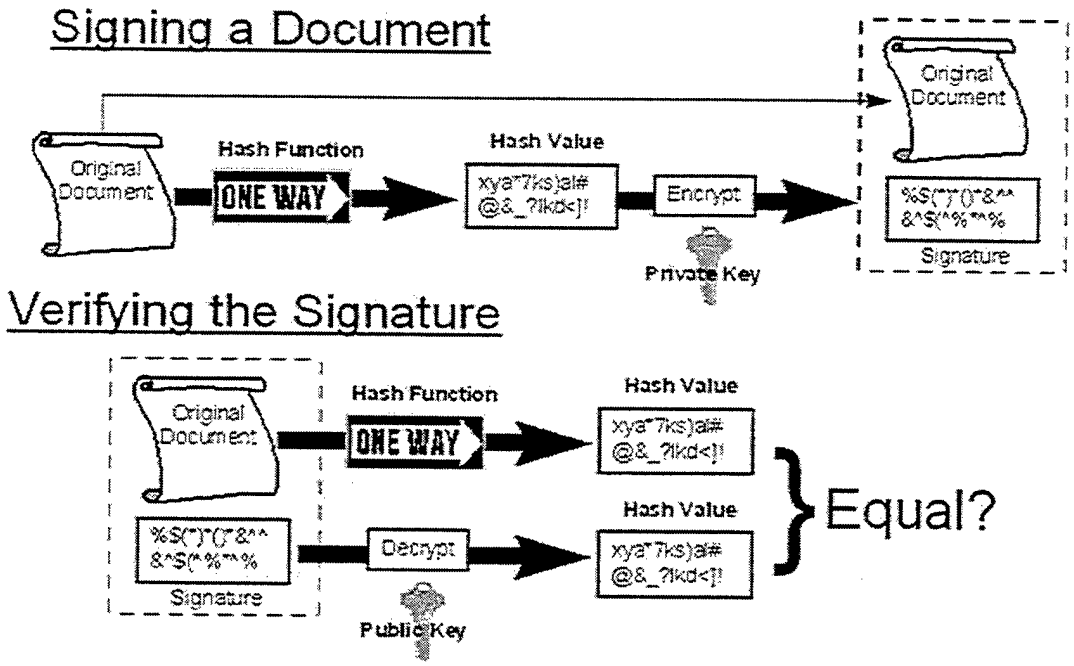


Figure A-3. Digital Signature. [From Ref. 11]

a. Message Authenticity

If the sender has kept his or her private key secure and if a digital signature of a message correctly verifies using the sender's public key, there is great assurance that the digitally signed message is from the owner of the private key. If a private key is compromised, digital signatures can easily be forged. Even if a mechanism exists for revoking the public keys that correspond to compromised private keys, forged digital signatures will be still accepted as valid in the time frame between the key was compromised and when the key was reported as compromised.

b. Message Integrity

Message integrity is another property digital signatures provide. If the digital signature of a message correctly verifies, then the hash of the received message is equal to the hash encrypted by the message sender. Since it is computationally infeasible to find two messages that hash to the same value, the two messages (the message hashed by the sender and the message hashed by the receiver) must be identical, thereby establishing message integrity.

c. Message Nonrepudiation

A message is nonreputable if the sender cannot deny sending it. If a message is digitally signed, the message is nonreputable, because it can be established that the hash of the message was encrypted with the sender's private key. Unless the sender can successfully argue that someone else has his or her private key, the sender is responsible for sending the message.

3. Confidentiality with Digital Signatures

Figure A-4 shows the steps involved in sending and receiving a message encrypted for confidentiality and digitally signed for authenticity, integrity, and nonrepudiation.

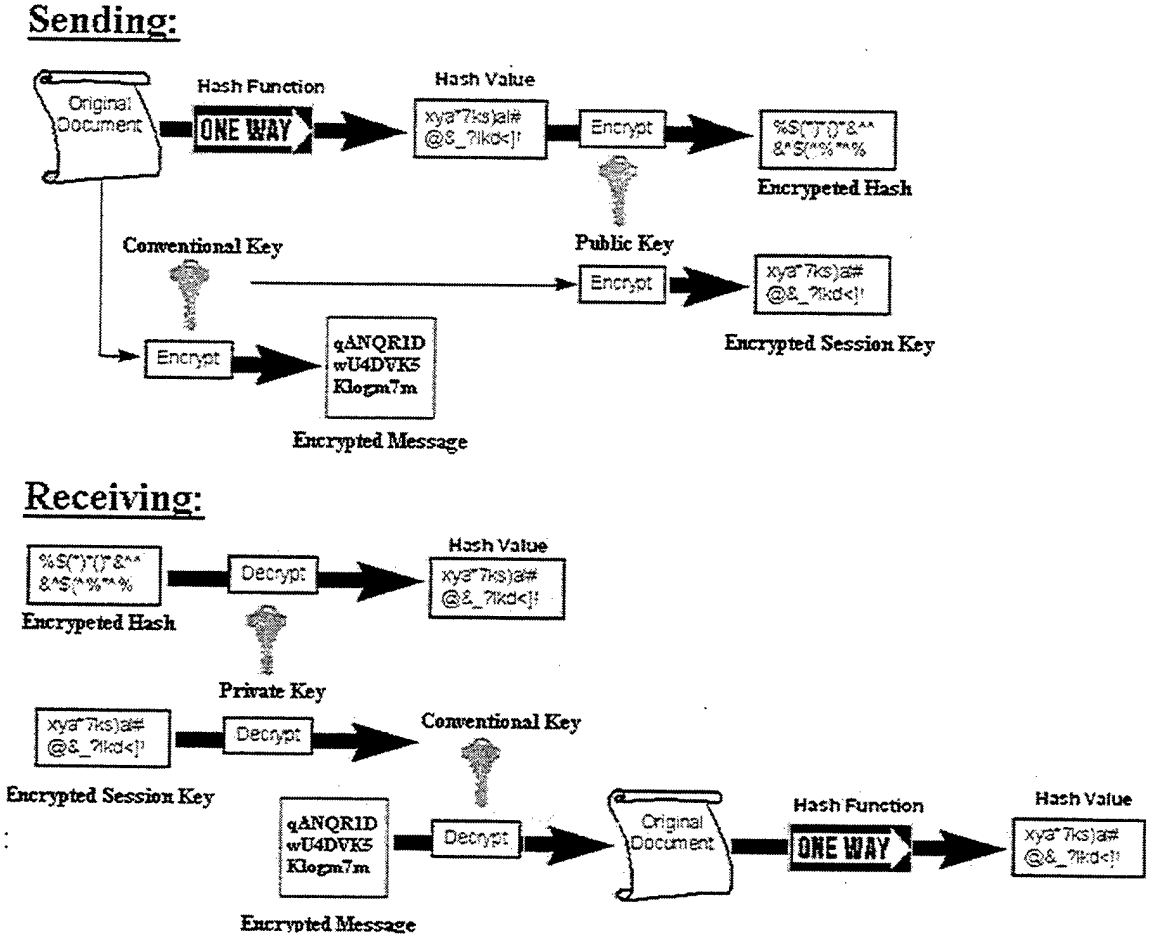


Figure A-4. Confidentiality with Digital Signatures. [After Ref. 11]

C. A PUBLIC KEY INFRASTRUCTURE

A public key infrastructure provides for the management of public and private keys. This management involves the secure generation and protection of an individual's private key and the authentic distribution of his or her public key. A public key infrastructure consists of many parts. The following is a description of the major components of a PKI.

1. Certificates and the X.509 Standard

Certificates were developed to handle the authentic distribution of public keys. They contain a public key and personal identification for an individual (or an entity such as an organization, account, or site). In essence, certificates provide an association between a public key and an individual. To protect this association, the certificate is digitally signed by a Certificate Authority (CA). [Figure A-5] CAs are further discussed in the next section.

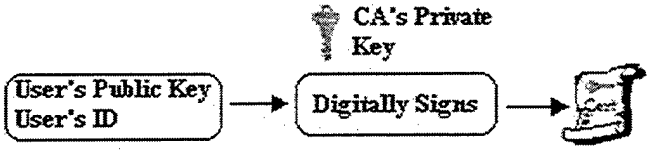


Figure A-5. Certificate.

Having the certificate digitally signed by a CA gives the user of the certificate a sense of confidence that the public key contained in the certificate belongs to the person or entity identified in the certificate. The certificate is also issued with a validation time period, so that new certificates are required at some predetermined time. The validation time period helps ensure that certificates are kept up-to-date and secure. The performance metric that measures the time to generate a certificate under the Navy Marine Corps Intranet requirements is evaluated in the performance measures section.

Table A-1. X509 V3 Certificate. [After Ref. 9 & 23]

Version	Version number; an integer, value is "2" for version 3	
Serial Number	Unique identifier for each certificate generated by issuer (CA); (An integer)	
Signature Algorithm ID	Algorithm identifier	Algorithm used to sign certificate (e.g. RSA with SHA-1)
	Parameters	Should not be used
Issuer name	Name of issuer (X.500 "distinguished name" (DN) that uniquely identifies a director object)	
Validity period	Not Before	When the certificate becomes valid
	Not After	Expiration date of certificate
Subject Name	Name of subject (X.500 "distinguished name") ("user")	
Subject public key information	Algorithm identifier	Subject's signature algorithm
	Parameters	Parameters applicable to subj. pub. Key
	Public key	Subject's public key
Issuer unique identifier	(optional) contains additional information about the issuer (CA) To prevent the reuse of issuer name over time.	
Subject unique identifier	(optional) contains additional information about the subject. To prevent the reuse of subject name over time.	
Extensions	Optional	Additional info about the certificate
Issuer's Signature	Algorithm identifier	Algorithm used for this signature
	Parameters	Should not be used
	ENCRYPTED (certificate hash)	

The DOD has chosen the X.509 Version 3 (X.509 v3) standard as the format for its certificate. Table A-1 provides a breakdown of the contents of a certificate.

The X.509 v3 extension fields allow for the addition of organization specific attributes.

2. Certificate Authorities and Registration Authorities

The process of generating a private key/public key pair requires a significant amount of security. Since the private key is used for digital signatures, it should never be exposed to anyone other than the user. The authenticity of the public key needs to be protected until the CA signs the certificate. While the CA is ultimately responsible for guaranteeing the identity of individuals during the certificate creation process, this responsibility is often delegated to a Registration Authority (RA) or a Local Registration Authority (LRA).

3. Certificate Creation

The first step in all certificate creation scenarios involves the user visiting an LRA, RA or CA and providing proof of his or her identity (Military ID, passport, driver's license, etc). The depth of the authentication process depends on the level of security required for the certificate. After the user authentication phase, a number of scenarios exist for the key creation process. Currently, a common process uses the LRA workstation to create a user's private and public keys. The LRA then transfers the user's private key to a floppy disk for the user and transfers the user's public key, ID, and information (via a Secure Socket Layer (SSL) channel) to the certificate authority, where the certificate is signed. The certificate is then stored in a certificate directory and can be distributed to the user via e-mail or on a floppy disk from the LRA. Future scenarios will use smart cards for private key/public key generation and private key storage. The DON will issue smart cards to all Navy and Marine Corps personnel by October 2001. The time required for a Navy/Marine Corps Intranet user to have a new certificate created is analyzed in greater detail in the performance measures section of this thesis.

4. Root Certificate Authority

Due to the hundreds of thousands of Navy and Marines Corps users that will require certificates, it would be impractical for only one certifying authority to distribute and manage the certificates for every N/MCI user. To assist in this endeavor, the root CA will establish subordinate CAs in a hierarchical structure, with the root CA at the top level of the hierarchy. The root CA issues certificates to subordinate CAs who will, in turn, use their certificates to issue certificates to members. [Ref. 21] The use of a hierarchical structure creates a certification path between the end user and the root CA. This method, unfortunately, allows for a major point of failure. Specifically, if the root CA's private key were to fall into untrustworthy hands, it would compromise the entire system. Since the National Security Agency (NSA) is the root CA for all certificates used by the N/MCI, it will monitor how the N/MCI contractor manages N/MCI certificates.

5. Interim External Certificate Authorities

The DOD heavily depends on using commercial products and services to conduct day-to-day business. This dependency requires that the military be able to communicate securely with its suppliers. To support this secure communication, the DOD will use Interim External Certificate Authorities (IECA). These Certificate Authorities will produce digital certificates for commercial contractors so they may securely communicate and contract with the government using the DOD PKI. These certificates are used with Electronic Commerce applications in the DOD. [Ref. 22] So far the DOD has approved the following IECAs:

- Digital Signature Trust (DST).
- Operation Research Consultants Inc. (ORC).
- Verisign.
- General Dynamics.

6. Certificate Directories

Certificate directories are an essential element of a PKI. Many PKI-enabled applications require the application to obtain the certificate for another entity. The certificate directory provides the repository for these certificates, and for other important PKI information such as Certificate Revocation Lists (CRLs). Usually, a separate directory server is created to keep this valuable information isolated from other functions. These directories are typically accessed through the Lightweight Directory Access Protocol (LDAP), which runs over Transmission Control Protocol/Internet Protocol (TCP/IP).

7. Trust in a Certificate / Certificate Authority

With the widespread use of PKI technology in the civilian and military communities, it is likely that it will attract the attention of the same undesirable individuals the system was created to keep out. There are several scenarios that could lead to possible security hazards if the PKI is not managed correctly. The scenario described below illustrates a flawed PKI that is not based on certificates. In this scenario, users distribute their public keys by posting them on electronic bulletin boards.

A malicious entity posts a public key on a bulletin board, under the name of Alice. He or she then sends a digitally signed message to Dave pretending to be Alice

using a digital signature that was created with the private key associated with the malicious public key posted on the bulleting board. When Dave verifies the digital signature using the public key on the bulletin board, he will think that the message is from Alice. Dave now has a false sense of trust because this public key is not really Alice's public key. This is just one example of a flawed PKI implementation. It is the responsibility of the N/MCI contractor to ensure that the required security measures are taken. The government is responsible for ensuring that the contractor is doing its job. SLA 34 performance measures support this responsibility.

8. Certificate Revocation List (CRL)

A certificate revocation list is a list of the certificates revoked due to the loss of a user's private key. This loss may be due to a number of problems. It could result from a malicious user getting access to another user's private key or it could be something as simple as a user forgetting the password that is used to protect their private key on their personal computer. The DOD standard for CRLs is X.509 v2. The data fields of an X.509 v2 CRL are shown in Table A-2. The DOD is a very transitive community, and it is likely that certificates may be canceled routinely. These routine cancellations have to be frequently distributed to the entire community so members can ensure the credibility of certificates. If there is a long time lapse between when a member leaves and when his certificate is added to the certificate revocation list, it could cause a security risk. The performance measures section analyzes the revocation process and the time the contractor takes to revoke certificates.

Table A-2. Revocation List. [After Ref. 9 & 23]

Signature	Algorithm identifier	Algorithm used to sign the CRL
	Parameters	Any parameters needed
Issuer	Name of CRL issuer (X.500 "distinguished name")	
This update	Time	Date & time the CRL was issued
Next update	Time	(Optional) date & time of next update
Revoked certificates	List of revoked certificates	
CRL extensions (optional) zero or more extensions	Criticality flag	If "true" extension must be processed
	Extension parameter	
Issuer's signature		

Serial number	Serial number of revoked certificate (unique for the issuer)	
Revocation date	Time	
CRL entry extensions (optional) zero or more extensions	Criticality flag	If "true" extension must be processed
	Extension parameter	

Another concern caused by having so many transient members is the sheer quantity of revoked certificates on the CRL. Every time a member uses a public key, the member will have to verify that the key is still valid (i.e. that the corresponding private key has not been compromised). Large CRLs will undoubtedly create a time delay in the verification process. One approach that can reduce the verification time is to segment the CRLs into revocation categories. For example, one CRL might only list routine revocations (e.g., user forgot password), and another CRL might list compromised keys (e.g., user's key was stolen). These lists could be sent out at different frequencies, with the compromised key CRL being more frequent. This way, if the user is only concerned

with the possibility of a compromised key, they will only have to verify the given certificate using the compromised key CRL. This process will not take as long as verifying certificates using a full CRL. [Ref. 12]

Another problem created by large CRLs is that they take up a lot of bandwidth during distribution. This problem can be addressed by the use of delta-CRLs. A delta-CRL is a list of the keys that have been revoked since the last time a full CRL or delta-CRL was issued. The general scheme will probably be to distribute the full CRLs less frequently and issue the delta-CRLs more frequently.

Another approach to the certificate revocation problem is the use of online certificate revocation. Online revocation is similar to credit card verification and provides real-time verification that the private key corresponding to a given certificate has not been revoked. Online revocation is based on the Online Certificate Status Checking Protocol, which will likely be an Internet standard in the future. This protocol has two significant characteristics: first, it depends on the emergence of its own three-tier (Client – CA – Designated Responder) infrastructure; second, it defines a new set of message formats extending beyond those contained in the base PKI X.509 v2 standard. [Ref. 15] Even though online revocation may simplify the process of certificate verification, it comes with a performance penalty (i.e., network congestion).

Please refer to the references for additional information.

LIST OF REFERENCES

1. *Performance Measures*, http://dizzy.library.arizona.edu/library/teams/slrp/syllabus/measure.html
2. *Navy/Marine Corps Intranet Contract*, Solicitation No. N00024-00-R-6000, Naval Sea Systems Command
3. *How was NMCI Developed?*, http://www.peo-it.navy.mil/nmci_develop.html
4. *NMCI Overview*, http://www.peo-it.navy.mil/nmci_overview.html
5. Mayo, Richard, Rear Admiral, *Statement to Congress*, March 8, 2000, http://www.house.gov/hasc/testimony/106thcongress/00-03-08mayo.htm
6. Warren, Dan, *Introduction to Computer Security*, Course Notes for CS3600, Naval Postgraduate School, Spring 2000
7. Michelsen, Christopher, J., *United States Navy Implementation of Department of the Defense (DOD) Public Key Infrastructure (PKI)*, September 1999
8. Denning, Dorthy, E., *Information Warfare and Security*, Association for Computing Machinery, Inc. July 1999
9. Gaines, Lenoard, T., *Trust and its Ramifications for the DOD Public Key Infrastructure (PKI)*, September 2000
10. Memorandum from the Assistant Secretary of Defense, *Department of Defense (DOD) Public Key Infrastructure (PKI)*, August 12, 2000
11. Galik, Dan, PKI and the Navy, January 2000 CHIPS magazine. http://www.norfolk.navy.mil/chips/archives/00_jan/pki.htm
12. *Basic Public-Key Infrastructure Characteristics*, A Survey of Public Key Infrastructure, http://home.xcert.com/~marcnarc/PKI/thesis/characteristics.html
13. Chokhani, S. & Ford, W., *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, The Internet Society 1999, http://www.imc.org/rfc2527
14. Fox, Barbara, & LaMacchia, Brian, *Online Certificate Status Checking in Financial Transactions: The Case for Re-issuance*, http://www.farcaster.com/p;apers/fc99/fc99.htm
15. Menez, Marty CAPT, *Navy/Marine Corps Intranet*, http://www.navres.navy.mil/navresfor/n6/99itsummit/nmci/sld012.htm
16. *NMCI Report to Congress* – 30 June 2000
17. Murry, Bill, *Joining Forces, The Navy and the Marine Corps have connected to launch one of the biggest technology outsourcing contracts ever*, *http://www.govexec.com/features/1200/1200s3.htm*

18. *Entrust Technologies Provides PKI Foundation for United States Federal Bridge Certification Authority,* Separate Pilots Prove Interoperability of Digital Signatures, http://www.entrust.comnews/files/04_10_00.htm 10 April 2000

19. *Public Key Infrastructure Implementation Plan for the Department of Defense,* Version 3.1, 18 December 2000

20. Hale, Richard, *Public Key Infrastructure (PKI) and the Use of Cryptography for Automating and Securing DOD Business Process,* 28 January 2000

21. Aresenault, A. & Turner, S., *draft-ietf-pkix-roadmap-06.txt*, November 2000

22. *DOD Approved IECA's*, http://eda.ogden.disa.mil/registration/DoD-IECAS.html

23. Housley, R & Ford, W. & Polk, W. & Solo, D., *RFC2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, http://www.ietf.org/rfc/rfc2459.txt January 1999

24. Kreisher, Otto, *Breaking Down the Barriers, Navy-Marine Corps Intranet: Speed, Flexibility, Security*, http://www.navyleague.org/seapower/breaking_down%20the_barriers.htm

25. Styles, Michael, B., *Federal Managers Association letter to Chairman for Senate Committee on Armed Services*, http://www.fedmanagers.org/mstyles_warner_oppose_nmci.htm , May 3, 2000

26. Defense Link, U.S. Department of Defense News, *Contracts Navy,* http://www.defenselink.mil/news/Oct2000/b10062000_bt618-00.html, October 6, 2000

27. E-mail between Donald Endicott, N/MCI Program Manager, SPAWAR and the author, on December 19, 2000

28. E-mail between Armand Gladu, SPAWAR N/MCI Green Team Leader and the author, on November, 30 2000

29. E-mail between Chris Harrington, Senior PKI Consultant CertCo, Inc and the author, on February 8, 2001

30. E-mail between Craig Sims, NCR DISA and the author, on February 1, 2001

31. E-mail between Bob Zagueneh, Litronic representative and the author, on February 1, 2001

32. E-mail between Netlock Technologis Inc representative and the author, on February 1, 2001

33. E-mail between Kym Mirabella, Eccelerate representative and the author, on February 8, 2001

34. E-mail between Digital Signature Trust representative and the author, on February 8, 2001

35. Lecture on *"A Performance Evaluation Study of an X.509 Compliant PKI"*, by Dr. Emilia Rosti, on February 22, 2001

36. E-mail between Gartner Group and the author, on February 1, 2001

37. Interview between Professor Daniel Warren and the author, on April 19, 2001

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Road, Suite 0944
   Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Road
   Monterey, CA 93943-5101

3. Professor Daniel Warren (Code CS/WD) 1
   Naval Postgraduate School
   Monterey, CA 93943-5002

4. Professor Carl R. Jones (Code IS/JS) 1
   Naval Postgraduate School
   Monterey, CA 93943-5002

5. Professor Dan Boger (Code IT/BO) 1
   Naval Postgraduate School
   Monterey, CA 93943-5002

6. Space and Naval Warfare System Command (SPAWAR) 1
   Contracting Officer: 02-32 Ellen H. Pollen
   4301 Pacific Highway, OT-4, Room 2082B
   San Diego, CA 92110-3127

7. Commander Robert Vassian 1
   16 High Bluff Dr.
   Weaverville, NC 28787

8. Lieutenant Randy A. Gumke 1
   U.S. Naval Mobile Construction Battalion ONE
   Unit 60251
   FPO AA 34099-4900